日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００２年１２月２５日

出願番号
Application Number: 特願２００２－３７５１２３

[ST. 10/C]: [ＪＰ２００２－３７５１２３]

出願人
Applicant(s): 株式会社日立製作所

２００４年 ２月 ５日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

出証番号 出証特２００４－３００６３１４

【書類名】　特許願

【整理番号】　HK14713000

【提出日】　平成14年12月25日

【あて先】　特許庁長官　殿

【国際特許分類】　H04L　9/16

【発明者】

【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内

【氏名】　水谷　美加

【発明者】

【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内

【氏名】　神牧　秀樹

【発明者】

【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内

【氏名】　海老名　明弘

【特許出願人】

【識別番号】　000005108

【氏名又は名称】　株式会社　日立製作所

【代理人】

【識別番号】　100084032

【弁理士】

【氏名又は名称】　三品　岩男

【電話番号】　045(316)3711

【手数料の表示】

【予納台帳番号】　011992

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】ネットワーク機器、ネットワークシステム、および、グループ管理方法

【特許請求の範囲】

【請求項１】

ネットワークを介して接続された他のネットワーク機器と通信を行なうネットワーク機器であって、

互いに認証可能な前記ネットワーク機器をグループとして管理するグループ管理手段と、

前記グループ所属するネットワーク機器間で共通の暗号化鍵による暗号通信を行う暗号通信手段と、

前記暗号化鍵の情報と前記グループに所属するネットワーク機器のホスト名およびアドレスを含む識別情報とを含む、前記グループに所属するネットワーク機器と暗号通信を行うために必要な暗号通信情報を格納する記憶手段と、

外部から情報を取得する取得手段と、を備え、

前記グループ管理手段は、

前記記憶手段に前記暗号通信情報が格納されていない状態で、前記取得手段において前記暗号通信情報を取得すると、当該暗号通信情報を前記記憶手段に格納するとともに、前記暗号通信手段を介して自身の識別情報を前記グループに所属するネットワーク機器に送信し、

前記暗号通信手段を介して他のネットワーク機器から当該他のネットワーク機器の識別情報を取得すると、前記記憶手段に記憶している前記暗号通信情報に当該識別情報を追加する

ことを特徴とするネットワーク機器。

【請求項２】

請求項１記載のネットワーク機器であって、

前記グループ管理手段は、さらに、

前記取得手段においてグループから離脱する指示を受け付けると、前記記憶手段に記憶されている前記グループに所属する全てのネットワーク機器に、前記暗

号通信手段を介して自身のネットワーク機器の離脱を通知するとともに、前記記憶手段から前記暗号通信情報を削除し、

前記暗号通信手段を介して他のネットワーク機器から、当該他のネットワーク機器が離脱する通知を受け付けると、前記記憶手段に記憶している前記暗号通信情報から、当該他のネットワーク機器の識別情報を削除する、

ことを特徴とするネットワーク機器。

【請求項３】

請求項１または２記載のネットワーク機器であって、

前記取得手段は、記憶媒体のインタフェースであり、

前記グループ管理手段は、さらに、

前記記憶手段に前記暗号通信情報が格納されている状態で、前記暗号通信情報が格納された記憶媒体が前記取得手段に挿入された場合、前記記憶手段に格納されている暗号通信情報を前記記憶媒体にコピーすること

を特徴とするネットワーク機器。

【請求項４】

請求項１、２、または、３記載のネットワーク機器であって、

非暗号通信を行なう非暗号通信手段と、

前記ネットワーク機器が提供するサービスに対するアクセスを制御するアクセス制御手段とをさらに備え、

前記アクセス制御手段は、前記非暗号通信手段を介して他のネットワーク機器からアクセスがあった場合、前記アクセスが予め定められたポートに対するものである場合、前記アクセスを許可すること

を特徴とするネットワーク機器。

【請求項５】

複数のネットワーク機器と、前記複数のネットワーク機器を接続するネットワークとを備えたネットワークシステムにおいて、

前記複数のネットワーク機器は、請求項１～４記載のネットワーク機器であることを特徴とするネットワークシステム。

【請求項６】

ネットワークを介して接続された他の機器と、互いに認証可能な暗号通信を行なうグループを管理するグループ管理方法であって、

前記ネットワークに接続された一つの機器において、前記暗号通信に用いる暗号化鍵を生成し、当該暗号化鍵と自機器のホスト名とアドレスとを含む識別情報とを暗号通信情報として保有するグループ生成ステップと、

前記暗号通信情報を取得した機器において、前記暗号通信情報に前記識別情報が格納されている全機器に自身の識別情報と参加を示す情報とを前記暗号通信により通知し、当該暗号通信情報に自身の識別情報を追加して保有する第１のグループ参加ステップと、

当該識別情報と前記参加を示す情報とを受けた機器において、自身が保有する前記暗号通信情報に当該識別情報を追加する第２のグループ参加ステップと、

前記グループから離脱する指示を受け付けた機器において、自身を除く前記暗号通信情報に前記識別情報が格納されている全機器に離脱を示す情報と自身の識別情報とを前記暗号通信により通知し、自身の保有する前記暗号通信情報を削除する第１のグループ離脱ステップと、

当該離脱の通知を受けた機器において、自身が保有する前記暗号通信情報から通知を受けた識別情報を削除する第２のグループ離脱ステップと、

を備えることを特徴とするグループ管理方法。

【請求項７】

コンピュータを、

暗号通信に用いる暗号化鍵を生成し、当該暗号化鍵と自身のホスト名およびアドレスを含む識別情報とを暗号通信情報として保有するグループ生成手段と、

前記暗号通信情報を取得すると、前記暗号通信情報に前記識別情報が格納されている全機器に自身の識別情報と参加を示す情報とを前記暗号通信により通知し、前記暗号通信情報に前記自身の識別情報を追加して保有する第１のグループ参加手段と、

他の機器から当該機器の識別情報と参加を示す情報とを受信すると、自身が保有する前記暗号通信情報に当該識別情報を追加する第２のグループ参加手段と、

前記暗号通信情報を削除する指示を受け付けると、自身を除く前記暗号通信情

報に前記識別情報が格納されている全機器に離脱を示す情報と前記自身の識別情報とを前記暗号通信により通知し、自身の保有する前記暗号通信情報を削除する第１のグループ離脱手段と、

他の機器の識別情報と前記離脱を示す情報とを受信すると、自身が保有する前記暗号通信情報から受信した識別情報を削除する第２のグループ離脱手段、

として機能させるためのプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ネットワークに接続する特定の機器間で排他的かつ安全に通信を行う技術に関する。

【０００２】

【従来の技術】

Internet Protocol（以下、ＩＰと呼ぶ）と呼ばれる通信プロトコルを使用するＩＰネットワークは、コンピュータネットワークのデファクトスタンダードとしての地位を確立し、一般ユーザへの普及が著しい。

【０００３】

このＩＰネットワークを介して機器間でデータをやりとりするには、その機器それぞれに一意的にＩＰアドレスを付与することが必要である。現在では、ＩＰアドレスを３２ビットで表すＩＰｖ４(Internet Protocol version 4)が用いられているが、ＩＰネットワークの利用が増大するに連れて、ＩＰアドレスの不足が大きな問題となってきている。

【０００４】

このような状況を背景に、ＩＰアドレスを１２８ビットに拡張し、さらに、セキュリティ機能など、今までのＩＰアドレスになかった機能を付加した新しいＩＰアドレスを用いるＩＰネットワークとしてＩＰｖ６(Internet Protocol version 6)がＩＥＴＦ(Internet Engineering Task Force)にて採択され、それを用いたネットワークサービスが次世代ＩＰとして標準化されつつある。

【０００５】

さらに、使用可能なアドレス数が増え、セキュリティ機能が充実したＩＰｖ６の新たな適用先として、冷蔵庫、洗濯機などの白物家電、あるいはテレビ、ビデオといったAV機器といった家庭内の機器から構成されるホームネットワークなどが注目されている。

【０００６】

これらの機器それぞれにＩＰアドレス割り当てることにより、各機器をサーバとみなすことができるようになり、機器間通信により新しいサービスを実現したり、外部端末からの機器の制御、サービスセンタからの機器の制御といったインターネットを介した新しいサービスを実現するといったことが考えられている。

【０００７】

ところで、家庭内機器のような特定の機器間の通信においては、利用者が認識している範囲外の機器からの操作を排除するようなシステムが要求される。例えば、友人が持ってきた機器による勝手な操作の防止が必要である。

【０００８】

すなわち、利用者が互いの通信を許可する範囲を決定し、それらの機器をグループ化し、グループ化された機器間でのみ通信がなされるようなシステムが要求される。そして、このような通信を実現するためには、グループ内の機器間で、互いをグループ内に属する真正な機器であることを認証するための認証機能が必要である。

【０００９】

このような認証機能として、従来のクライアント、サーバ型のシステムでは、認証サーバを用いたものが実現されている。例えば、ＲＦＣ２８６５で定義されるＲＡＤＩＵＳ(Remote Authentication Dial-In User Serviceでは、サーバにアクセスするクライアントのアカウント（ユーザ名、パスワード）をＲＡＤＩＵＳサーバと呼ばれる認証サーバで一括管理し、サーバは、クライアントからのアクセス要求(ユーザ名点パスワードを含む)をＲＡＤＩＵＳサーバに転送しアクセス可否の判断結果を受けて、クライアントとの通信を行うかどうか判断する。

【００１０】

例えば、従来のグループ化された特定の機器間での暗号通信システム及びその

通信方法としては、特開２００２-１２４９４１号公報（特許文献１）及び特開平５－３４７６１６号公報（特許文献２）に示されているものがある。

【特許文献１】特開２００２－１２４９４１号公報

【特許文献２】特開平５－３４７６１６号公報

【発明が解決しようとする課題】

ホームネットワークに接続されている機器の中で、利用者が指定した機器間でのみ所定の通信を行うためには、互いに相手が指定された機器であることを認証する機能が必要と考えられている。

【００１１】

従来の認証機能は、クライアント・サーバシステムが前提であり、サーバにアクセスするクライアントのアクセス情報を管理する認証サーバを備えることで実現されている。

【００１２】

これに対し、ホームネットワークを構成する機器は、適宜サービスに応じて必要な機器間で通信を行なうといったアドホック型である。このため、全ての機器がサーバにもクライアントにもなり得、アクセス情報の設定がより煩雑になるという問題がある。

【００１３】

このような場合に、従来のように認証サーバを備え、機器間でのセッション確立毎、あるいはサービス開始毎に個別に認証を行うようにすると、認証のオーバヘッドが大きくなるという問題もある。

【００１４】

例えば、前述の特許文献１に開示された技術は、認証機能を有したグループ通信システムである。本技術は、グループを構成する機器以外に、グループ通信システム内にグループ暗号鍵を生成する機能及びグループに所属する端末情報を管理する機能を備えたグループ暗号鍵管理部と及び中継装置とを備えて構成され、大規模なネットワーク構成を前提としたものである。

【００１５】

また、前述の特許文献２に開示された技術は、まず、グループ通信を行う機器

ごとにＩＣカードを具備していなければならない。そして、そのＩＣカードには、予め送受信相手の所属ごとに設定された複数のマスタ鍵とグループ鍵生成プログラムとが記録されている必要がある。

【００１６】

このように、従来の技術では、実際に通信を行なう機器以外に認証サーバとなる機器を用意する必要があったり、マスタ鍵と個々の通信相手先の関係といった複雑な情報を予め記憶させておく記録媒体をグループを構成する機器の数だけ用意する必要があった。

【００１７】

本発明は、このような事情に鑑みなされたもので、本発明の目的は、利用者が認めた機器間で容易に互いを認証し合うことが可能なグループを構成し、そのグループに属する機器間の安全な通信を実現することにある。

【００１８】

さらに、本発明の他の目的は、グループ内の機器が提供するアプリケーションにグループ外の機器にもアクセスを許可するものがある場合、グループ外の機器から、そのアプリケーションにのみアクセスを許可するといったアクセス制御を実現することにある。

【００１９】

【課題を解決するための手段】

本発明は、共有の鍵を用いて暗号通信を行うことで互いを認証し、セキュリティの確保された通信を行なう機器の集まりをグループとみなし、そのグループを構成する機器となりうる個々の機器のいずれもが、グループを生成し、参加し、また、そのグループから離脱するといったグループ管理の手段を有する。

【００２０】

また、機器がいずれかのグループに属していても、グループ外の機器との通信の可能性も保有するものである。

【００２１】

具体的には、ネットワークを介して接続された他のネットワーク機器と通信を行なうネットワーク機器であって、互いに認証可能な前記ネットワーク機器をグ

ループとして管理するグループ管理手段と、前記グループ所属するネットワーク機器間で共通の暗号化鍵による暗号通信を行う暗号通信手段と、前記グループに所属するネットワーク機器の、ホスト名とアドレスとを含む識別情報および前記暗号化鍵の情報を含む前記グループに所属するネットワーク機器と暗号通信を行うために必要な暗号通信情報を格納する記憶手段と、外部から情報を取得する取得手段と、を備え、前記グループ管理手段は、前記記憶手段に前記暗号通信情報が格納されていない状態で、前記取得手段において前記暗号通信情報を取得すると、当該暗号通信情報を前記記憶手段に格納するとともに、前記暗号通信手段を介して自身の識別情報を前記グループに所属するネットワーク機器に送信し、前記暗号通信手段を介して他のネットワーク機器から当該他のネットワーク機器の識別情報を取得すると、前記記憶手段に記憶している前記暗号通信情報に当該識別情報を追加することを特徴とするネットワーク機器を提供する。

【００２２】

また、前記グループ管理手段は、さらに、前記取得手段においてグループから離脱する指示を受け付けると、前記記憶手段に記憶されている前記グループに所属する全てのネットワーク機器に、前記暗号通信手段を介して自身のネットワーク機器の離脱を通知するとともに、前記記憶手段から前記暗号通信情報を削除し、前記暗号通信手段を介して他のネットワーク機器から、当該他のネットワーク機器が離脱する通知を受け付けると、前記記憶手段に記憶している前記暗号通信情報から、当該他のネットワーク機器の識別情報を削除する、ことを特徴とするネットワーク機器を提供する。

【００２３】

【発明の実施の形態】

以下、本発明の実施の形態を、図を用いて説明する。

【００２４】

本実施形態では、宅内において家電などにより構成されるネットワークに本発明を適用した場合を例にあげ、説明する。

【００２５】

本実施形態の宅内のネットワークは、ＩＰｖ６により構成され、それぞれにＩ

Ｐアドレスが付与された、例えば、電子レンジやエアコンなどの家電機器、テレビやビデオなどのAV機器、センサ等が接続されている。以下、ネットワークに接続され、ＩＰｖ６によるＩＰアドレスを付与されている各機器を、ノードと呼ぶこととする。

【００２６】

本実施形態では、これらのノードのうち、利用者が互いに通信を行なうことを許可したものをグループとし、グループに属するノード間で認証のために共通の暗号化鍵による暗号通信を行なう。

【００２７】

ここで、本ネットワークで採用しているＩＰｖ６は、前述したように、確保できるＩＰアドレス数が莫大となるだけでなく、ＩＰｓｅｃと呼ばれる暗号・認証の仕組みが標準で装備され、高度な安全性を保ちながら、使い勝手もよいという特徴を持つ。本実施形態においては、ＩＰｖ６のＩＰｓｅｃを用いて、グループを構成する機器間のみでの安全な通信を実現する。

【００２８】

本実施形態の詳細な説明の前に、まず、ＩＰｓｅｃの概要について説明する。ＩＰｓｅｃは、ＩＰ層において相互接続可能で高品質な暗号化ベースのセキュリティを提供する技術である。このセキュリティは、認証ヘッダＡＨ（Authentication Header）とＩＰ暗号化ペイロードＥＳＰ（Encapsulation Security Payload）の２つのトラフィックセキュリティプロトコル等によって実現されている。

【００２９】

ＡＨは、ＩＰパケットの改ざんを防ぐ機能を提供し、ＥＳＰは、ＩＰパケットを暗号化し、かつ、その認証データを格納することで、ＩＰパケットの機密性と完全性とを保証するものである。

【００３０】

ＡＨ、ＥＳＰ共に、認証鍵、暗号鍵を用いて、それぞれ認証情報、暗号データを作成し、送付した暗号化されたデータを解読可能な鍵を保有しているか否かにより通信相手の機器を認証する。

【００３１】

図４と図５とに、それぞれ、ＡＨプロトコルおよびＥＳＰプロトコルを利用した場合のＩＰパケットの構成を示す。なお、これらのパケット構成は、ＩＰｓｅｃパケットとしてＲＦＣ２４０１～２４０３に規定されているものである。

【００３２】

図４は、ＡＨプロトコルを利用した場合のＩＰパケットの構成を示すものである。この場合のＩＰパケットは、ＩＰヘッダ４００と、ＴＣＰ／ＵＤＰヘッダ４０２と、データ４０３に対するハッシュ値を格納するＡＨヘッダ４０１とを備える。

【００３３】

ＡＨヘッダ４０１に格納されているハッシュ値は、パケットが改ざんされていないことを証明するためのもので、通信相手間で相互に保有する認証鍵を用いて計算された値が格納される。これは、認証されているもの同士では同じ認証鍵を保有することが前提となっているもので、送信側で自身が保有する認証鍵によって計算して格納したデータのハッシュ値を、受信側が、自身が保有する認証鍵によって計算したデータのハッシュ値と比較し、両者が合致することにより、相手が同じ認証鍵を保有するものであることを確認することができる。すなわち、パケットの送信相手が同じ暗号化鍵を保有するグループ内の機器であることが証明される。

【００３４】

図５はＥＳＰプロトコルを利用した場合のＩＰパケットの構成を示すものである。ＴＣＰ／ＵＤＰヘッダと、データを暗号化した場合のヘッダ構成である。

【００３５】

この場合のＩＰパケットは、暗号化しているパケットであることを示すＥＳＰヘッダ５０１と、暗号化の区切りを揃えるためのＥＳＰトレーラ５０４と、認証データ５０５とを備える。認証データ５０５はオプションであり、ＥＳＰヘッダ５０５と、暗号化されたＴＣＰ／ＵＤＰヘッダ５０２と、データ５０３と、ＥＳＰトレーラ５０４とのハッシュ値を格納するものである。

【００３６】

認証データ５０５に格納されるハッシュ値は、ＩＰペイロードの完全性を確保

し、暗号化して転送するＴＣＰ／ＵＤＰヘッダ５０２およびデータ５０３の機密性を確保する。暗号化を行なう際には送信側が保有する暗号鍵を用いる。送信側が自身が保有する暗号鍵を用いて暗号化したデータを受信側は自身が保有する暗号鍵で復号する。受信側において、復号ができれば、相手が同じ暗号鍵を保有することが確認できる。すなわち、パケット送信相手が同じ暗号鍵を保有するグループ内機器であることの証明となる。

【００３７】

また、ＩＰｓｅｃで使用する暗号/認証アルゴリズム、鍵など、各機器間でＩＰｓｅｃの規格に従って通信を行う（以後、ＩＰｓｅｃの規格に従って行う通信のことをＩＰｓｅｃ通信と呼ぶ）ために共有すべき情報は、セキュリティアソシエーション(ＳＡ)として管理される。

【００３８】

ＳＡは、それによって運ばれるトラフィックに対してセキュリティサービスを提供する単方向の「コネクション」である。このため、ＩＰｓｅｃ通信を行うにあたって、通信を行う機器間で一方向の通信ごとに、予め設定を行う必要がある。すなわち、両方向の通信を行なうためには、送信方向と受信方向とのそれぞれのＳＡを設定する必要がある。

【００３９】

なお、ＩＰｓｅｃの詳細は、ＲＦＣ２４０１”Security Architecture for the Internet Protocol”に規定されている。

【００４０】

図１は、本発明を適用した一実施形態に係るグループ通信システムの構成を示す図である。

【００４１】

本図に示すように、本実施形態においては、４つのノード１００（１００Ａ、１００Ｂ、１００Ｃ、１００Ｄ）がＩＰｖ６によるネットワーク１１０に接続されている。もちろん構成ノード数はこれに限られない。

【００４２】

これらのノード１００間で、ネットワーク１１０を介してＩＰパケット形式の

コマンドを送受信することにより、ノード１００各々が備える機器特有のサービス機能に対する他のノード１００からの操作、および、他のノード１００へのサービス提供が実現される。

【００４３】

具体的には、ネットワークを介して、テレビからエアコンの温度調節をしたり、テレビからの操作により、ビデオカメラで撮影している画像をビデオに送信し、ビデオカメラで撮影した画像をビデオで録画させるといったことが実現されるものである。

【００４４】

例えば、ノード１００Ａ～ノード１００Ｃは、利用者が相互にサービスを利用することを許可しているグループに属するノードであり、ノード１００Ｄは、そのグループ外のノードとすると、グループを構成するノード１００Ａ、１００Ｂ、１００Ｃ間では、サービス機能の利用要求を送信する際に、要求元ノードは、グループで共有する鍵（以後、グループ鍵と呼ぶ）により計算されたハッシュ値を格納した、または、暗号化したＩＰパケットを送付する（１０１方向）。利用要求を受け取った要求先ノードは、自身の保有するグループ鍵により要求元ノードがグループ構成ノードであることを確認し、サービス機能を要求元ノードに提供する（１０２方向）、といったＩＰｓｅｃ通信を行なう。

【００４５】

これに対し、ノード１００Ｄからは、サービス機能の利用要求は、通常のＩＰパケットによって送信することとなるため、ノード１００Ｃに通常のＩＰパケットを送信すると（１０４方向）、ノード１００Ｃにおいてグループ外ノードと判断され、サービス提供拒否のパケットの返答を受けることとなる（１０３方向）。

【００４６】

ここで、ノード１００Ｂがグループ外のノード１００に提供を許可するサービスを有するノードの場合、ノード１００Ｄからそのサービスの提供を指定して通常のＩＰパケットを送信すると（１０４ｂ方向）、ノード１００Ｂよりそのサービスが提供される（１０３ｂ方向）。

【００４７】

本実施形態では、以上のようにＩＰｓｅｃの仕組みを標準で実装するＩＰｖ６を用いたプロトコルによる通信が可能なネットワークを例にあげて説明する。しかし、グループを構成するノード１００間に共通の暗号化鍵を持たせ、その鍵を認証鍵または暗号鍵として当該グループ間で通信を行うことができる環境を構築できるならば、通信プロトコルはこれに限られない。

【００４８】

以下、このようなネットワークに接続されたノード１００間で、所定のサービスの安全な利用を実現するグループの管理方法、すなわち、一つのノード１００においてグループを生成し、生成されたグループに他のノード１００が参加し、また、生成されたグループから離脱する方法について説明する。

【００４９】

本実施形態では、空のメモリカードＡ、Ｂの２つを用意し、最初にグループに参加するノード１００において、グループ内でＩＰｓｅｃ通信を行うために必要な情報を生成し、そのうちの一つのメモリカードＡに、登録する。その後参加するノード１００は、メモリカードＡから必要な情報を取得することで、グループに参加する。また、グループから離脱する際は、空のメモリカードＢを用いる。

【００５０】

図２にノード１００のハードウェア構成を、図３にその機能構成を示す。

【００５１】

ノード１００は、ノード１００が備える一つ以上の固有機能部２０２と、ネットワークカード２０５と、固有機能部２０２及びネットワークカード２０５を制御するプロセッサ２００と、プロセッサ２００で実行するプログラムを記憶するメモリ２０１と、プログラム及び設定情報を記憶するハードディスク等の外部記憶装置２０４と、グループ情報を受け渡すためのメモリカード等のインタフェースを提供する記憶媒体インタフェース２０６と、これらを接続するシステムバス２０３とを備える。

【００５２】

なお、固有機能部２０２が実現する固有機能とは、例えばエアコンであれば、

例えば冷暖房機能、温度管理機能、タイマ機能等を司る処理部などのことである。

【００５３】

また、記憶媒体インタフェース２０６は、挿入する記憶媒体に書き込み中であることを利用者に通知するＬＥＤ（発光ダイオード）ライトを具備している。

【００５４】

次に、各ノード１００が備える機能を図３に従って説明する。これらの機能により、ノード１００は、ネットワークを介して、利用者がサービスの相互利用を許可したグループを構成するノード１００間でサービスの提供を実現する。

【００５５】

各ノード１００は、アプリケーション３０１と、グループ管理処理部３０２と、ＴＣＰ／ＵＤＰ送信処理部３０３と、ＩＰ送信部３０４と、アクセスポリシデータベース３０８と、ＳＡデータベース３０９と、ネットワークインタフェース受信処理部３１０と、ＩＰ受信部３１４と、ＴＣＰ／ＵＤＰ受信処理部３１５と、ネットワークインタフェース送信処理部３１７と、記憶媒体インタフェース処理部３１８とを備える。

【００５６】

アプリケーション３０１は、各ノード特有のサービスを提供するものである。

【００５７】

グループ管理処理部３０２は、後述するグループの生成、離脱、更新など、グループに関する管理を行なうものである。

【００５８】

ネットワークインタフェース受信処理部３１０とネットワークインタフェース送信処理部３１７とは、ネットワークカードを制御するものである。

【００５９】

記憶媒体インタフェース処理部３１８は、記憶媒体インタフェース２０６を制御するものである。記憶媒体インタフェース３１８は、メモリカード等の記録媒体が記録媒体インタフェース２０６に挿入されたことを検出すると、記憶媒体インタフェース２０６に備えられているＬＥＤライトを点灯し、メモリカードを利

用中であることを利用者に対して示す。また、グループ管理処理部３０２から処理終了の通知を受けると、記憶媒体インタフェース２０６に備えられているＬＥＤライトを消灯し、利用者に対し、メモリカード等の記憶媒体への書込みが終了したこと、および、グループ管理処理部３０２における処理が完了したことを通知する。

【００６０】

なお、通知を受けた利用者は、メモリカードを当該記憶媒体インタフェース２０６から取り出すことができる。

【００６１】

ＴＣＰ／ＵＤＰ送信処理部３０３と、ＩＰ送信部３０４と、ＩＰ受信部３１４と、ＴＣＰ／ＵＤＰ受信処理部３１５とは、送受するＩＰパケットに対し、各層の処理を行い、通信を実現するものである。

【００６２】

ＩＰ送信部３０４は、ＩＰｖ６送信前処理部３０５と、ＩＰｓｅｃ送信処理部３０６と、ＩＰｖ６後処理部３０７とを備え、ＩＰ受信部３１４は、ＩＰｖ６受信前処理部３１１と、ＩＰｓｅｃ受信処理部３１２と、ＩＰｖ６受信後処理部３１３とを備える。ＩＰ送信部３０４とＩＰ受信部３１４とで、ＩＰｖ６による通信を実現する。

【００６３】

ここで、ＩＰｖ６受信前処理部３１１は、ＩＰヘッダを構成するバージョン、ペイロード長、ホップ・リミットの設定値の確認およびオプションヘッダ（ＡＨとＥＳＰとを除く）処理といったＩＰｖ６受信前処理を行なうものである。ＩＰｖ６受信前処理部３１１は、受け取ったＩＰパケットにＡＨヘッダまたはＥＳＰヘッダのいずれかが付加されていた場合、そのＩＰパケットをＩＰｓｅｃ処理部３１２に受け渡す。いずれのヘッダも付加されていなかった場合、そのＩＰパケットを後述する受信アクセス制御部３１６に受け渡す。

【００６４】

ＩＰｓｅｃ処理部３１２は、ＩＰヘッダのオプションヘッダのうち、ＡＨとＥＳＰの処理を行ない、受信したＩＰパケットがグループに属するノード１００か

ら送信されたものか否かを判断する。

【００６５】

ＩＰｖ６受信後処理部３１３は、ＩＰパケットを受け取ると、送信元ＩＰアドレス、送信先ＩＰアドレスを含むPusedo Headerを作成し、受け取ったＩＰパケットのＩＰヘッダと置き換え、ＴＣＰ/ＵＤＰ受信処理部３１５に受け渡すといったＩＰｖ６受信後処理を行なう。

また、ＩＰ受信部３１４は、受信アクセス制御部３１６をさらに備える。

【００６６】

受信アクセス制御部３１６は、ＩＰｖ６受信前処理部３１１から、ＡＨヘッダまたはＥＳＰヘッダを有していないＩＰパケットを受け取り、当該ＩＰパケットのアプリケーションへのアクセスを制御するものである。

【００６７】

ＳＡデータベース３０９は、ＩＰｓｅｃで必要なセキュリティアソシエーション（ＳＡ）が格納されているものである。

【００６８】

アクセスポリシデータベース３０８は、グループ内での通信を実現するため、各ノードに対するアクセス制御に関する情報及びグループ情報が格納されているものである。

【００６９】

アクセスポリシデータベース３０８は、グループ管理テーブル６００と、アクセス制御対象アプリケーション管理テーブル７００と、グループメンバ管理テーブル８００とを備える。

【００７０】

なお、グループ管理テーブル６００は、記憶媒体インタフェース２０６を介してノードに接続される記憶媒体であるメモリカード上でも保持されるものである。

【００７１】

以下、グループ管理処理部３０２、アクセスポリシデータベース３０６の各データベース、および、ＳＡデータベース３０９内のＳＡについて、その詳細を説

明する。

【００７２】

図６に、グループ管理処理部３０２の機能構成図を示す。

【００７３】

本図に示すように、グループ管理処理部３０２は、制御部３１００と、グループ生成処理部３２００と、グループ参加処理部３３００と、グループ離脱処理部３４００と、グループ情報更新処理部３５００と、グループ制御ＩＰパケット受信処理部３６００とを備える。

【００７４】

グループ管理処理部３０２は、ユーザがメモリカードを記憶媒体インタフェース２０６に挿入したことを検出した記憶媒体インタフェース処理部３１８からの指示で処理を開始する。

【００７５】

制御部３１００は、記憶媒体インタフェース処理部３１８からの指示を受け、挿入されたメモリカード内と、自身が保有するアクセスポリシデータベース３０８を検索し、グループ管理テーブル６００の有無を確認する。

【００７６】

グループ生成処理部３２００は、グループ自体が存在しない場合に、新たにグループを生成するグループ生成処理を行なう。グループ生成処理は、制御部３１００がメモリカードにもアクセスポリシデータベース３０８にもグループ管理テーブル６００が存在しないと判断した場合に行なわれるものである。

【００７７】

具体的には、グループに属する他のノードと暗号通信を行なうために必要な情報、すなわち、グループ管理テーブル６００に登録すべき項目を生成、選択し、グループ管理テーブル６００を作成し、それを、メモリカードおよびアクセスポリシデータベース３０８に登録する。

【００７８】

グループ参加処理部３３００は、既存のグループに、新たなメンバとして自身を参加させるグループ参加処理を行なうものである。グループ参加処理は、制御

部３１００がメモリカードにはグループ管理テーブル６００が存在するが、アクセスポリシデータベース３０８にグループ管理テーブル６００が存在しないと判断した際に行われるものである。

【００７９】

グループ参加処理部３３００は、挿入されたメモリカードに格納されている暗号通信に必要な情報を取得し、また、自身のノード１００と暗号通信を行なうために必要な情報をグループに既に属している他のノード１００に送信する。具体的には、メモリカード内のグループ管理テーブル６００に自身の情報を追加し、自身の情報が追加されたグループ管理テーブル６００を、アクセスポリシデータベース３０８に登録する。

【００８０】

また、グループ管理テーブル６００から得た、グループに既に属しているノード１００のホスト名からＩＰアドレスを解決することで、グループメンバ管理テーブル８００を生成する。

【００８１】

さらに、グループ参加処理部３３００は、グループ内の各ノード１００とＩＰｓｅｃ通信が可能となるように、セキュリティアソシエーションの設定を行ない、ＳＡデータベース３０９に登録し、グループ内の既存のメンバのノード１００に、ＩＰｓｅｃ通信で自身が追加されたことを通知する。

【００８２】

グループ離脱処理部３４００は、グループから離脱するグループ離脱処理を行なうものである。

【００８３】

本実施形態では、ユーザが所定のノード１００をグループから離脱させたい場合、当該ノード１００に空のメモリカードを挿入することとする。すなわち、グループ離脱処理は、制御部３１００が、自身のアクセスポリシデータベース３０８にはグループ管理テーブル６００が存在するが、挿入されたメモリカードにはグループ管理テーブル６００が存在しないと判断した際に行われるものである。

【００８４】

グループ離脱処理は、グループに属する他のノード１００に自身のノード１００が離脱することを通知し、当該グループ内で暗号通信を行なうために必要な情報、すなわち、自身のアクセスポリシデータベース３０８およびＳＡデータベース３０９内のグループ間の通信に係わるデータを削除するものである。

【００８５】

ここで、グループ参加処理部３３００およびグループ離脱処理部３４００がそれぞれ、参加および離脱をグループに属する各ノード１００に通知する際は、グループ制御ＩＰパケットと呼ぶ特別なデータ部を有するＩＰパケットを用いる。

【００８６】

ここで、そのグループ制御ＩＰパケットについて説明する。図７にグループ制御ＩＰパケットのデータ部１０００の一例を示す。

【００８７】

本図に示すように、グループ制御ＩＰパケットのデータ部１０００は、コマンド識別子を格納するコマンド識別子格納部１００１と、ＩＰアドレスとホスト名とをそれぞれ格納する、１６バイトのＩＰアドレス格納部１００２と、ホスト名格納部１００３とを備える。

【００８８】

ここで、新規参加を通知する際にグループに属する各ノード１００に送信されるグループ制御ＩＰパケットの場合、コマンド識別子格納部１００１に「加入」を示す（００）hexが設定される（以後、本グループ制御ＩＰパケットを加入コマンドと呼ぶ）。そして、ＩＰアドレス格納部１００２と、ホスト名格納部１００３とには、それぞれ自身のアドレスとホスト名とが設定される。

【００８９】

また、グループから離脱する際にグループに属する各ノード１００に送信されるグループ制御ＩＰパケットの場合、コマンド識別子格納部１００１に「離脱」を示す（０１）hexが設定される（以後、本グループ制御ＩＰパケットを離脱コマンドと呼ぶ）。そして、ＩＰアドレス格納部１００２と、ホスト名格納部１００３とには、それぞれ自身のアドレスとホスト名とが設定される。

【００９０】

グループ情報更新処理部３５００は、グループ管理テーブル６００の内容を更新したり、それをメモリカードにコピーするといったグループ情報更新処理を行なうものである。

【００９１】

本実施形態においては、セキュリティを向上させるために、グループ内で利用するグループ鍵が所定の期間ごとに更新される設定となっている。グループ情報更新処理部３５００は、グループ管理テーブル６００の鍵有効期限がタイムアウトした時点で、新しいグループ鍵を生成する。

【００９２】

ここで、グループ管理テーブル６００生成時に、ノード毎に、異なる鍵有効期限が設定される。具体的には、所定の有効期限の、例えば、プラスマイナス３０％間のランダムな値を、その鍵有効期限に加算あるいは減算することで得られた値を鍵有効期限として各ノードに設定する。このため、各ノードで鍵有効期限のタイムアウトが異なるタイミングで生じ、鍵の更新を行なうノードが一つに定まり、グループのメンバが同時にグループ鍵を生成することを避けることができる。

【００９３】

そして、更新されたグループ鍵を更新前のグループ鍵で暗号化し、グループ鍵を更新したメンバからグループに属する各ノードに送付する。このとき、鍵の更新とともに、各ノードの鍵有効期限を再設定してもよい。

【００９４】

また、グループ情報更新処理部３５００は、他のノードから、更新されたグループ鍵を受信した場合、自身の保有するグループ鍵の情報を更新するとともに、グループに属する各ノード１００のＩＰアドレスが更新された場合、関連するデータベース内のＩＰアドレスを更新する。

【００９５】

ここで、本実施形態では、グループの鍵の更新は上述のように行なわれるため、グループ参加処理に用いられるメモリカード内のグループ管理テーブル６００には反映されない。同様に、上述のグループからの離脱処理は、空のメモリカー

ドを用いて行なわれ、離脱したノード１００からグループを構成する他のノード１００への通知は、ＩＰｓｅｃ通信によって行われる。このため、グループ離脱によるグループ構成メンバの変更も、グループ参加処理に用いられるメモリカード内のグループ管理テーブル６００に反映されない。

【００９６】

このため、本実施形態では、グループ情報更新処理部３５００が、メモリカード内のグループ管理テーブル６００の更新処理も行なう。

【００９７】

グループ情報更新処理部３５００が行なうメモリカード内のグループ管理テーブル６００の更新処理は、制御部３１００が、自身のアクセスポリシデータベース３０８にも、挿入されたメモリカードにもグループ管理テーブル６００が存在すると判断した際に行われるものである。

【００９８】

グループ情報更新処理部３５００は、当該ノード１００のアクセスポリシデータベース３０８に格納されているグループ管理テーブル６００の情報をメモリカード内のグループ管理テーブル６００にコピーする。

【００９９】

本実施形態では、実際のグループ参加処理において、グループ参加処理を行なう場合に、グループに既に所属しているノード１００にメモリカードを挿入し、メモリカード内のグループ管理テーブル６００を最新のものとする処理を前もって行なうよう手順を定めておく。

【０１００】

グループ制御ＩＰパケット受信処理部３６００は、前述のグループ制御ＩＰパケットを受信した際の処理を行うものである。

【０１０１】

具体的には、加入コマンドを受信した場合は、ＩＰアドレス格納部１００２およびホスト名格納部１００３に格納されているＩＰアドレスおよびホスト名を自身のグループ管理テーブル６００およびグループメンバ管理テーブル８００とに追加し、送信元ノード１００と暗号通信を行なうために必要なセキュリティアソ

シエーションを作成する。一方、離脱コマンドを受信した場合は、それらを削除する。

【０１０２】

次に、アクセスポリシデータベース３０８に格納されるグループ管理テーブル６００とアクセス制御対応アプリケーション管理テーブル７００と、グループメンバ管理テーブル８００とについて以下に説明する。

【０１０３】

グループ管理テーブル６００は、グループに属するノード１００を識別するための情報とグループで共有する鍵の情報とを格納するテーブルである。図８にその一例を示す。

【０１０４】

本図に示すようにグループ管理テーブル６００は、ネットワークに接続されたノード１００によって構成されるグループを識別するためのグループ識別子を格納するグループ識別子格納フィールド６０１と、グループ鍵を格納するグループ鍵格納フィールド６０２と、そのグループ鍵の有効期限を格納するグループ鍵有効期限格納フィールド６０３と、ＡＨ、ＥＳＰといったグループ内で通信に利用するＩＰｓｅｃの機能の種別を格納するＩＰｓｅｃ種別格納フィールド６０４と、認証あるいは暗号に用いるアルゴリズムを格納するアルゴリズム格納フィールド６０５と、グループに属するノード１００を識別する情報であるホスト名を格納するホスト名格納フィールド６０６（６０６Ａ～６０６Ｂ）とを備える。

【０１０５】

アクセス制御対象アプリケーション管理テーブル７００は、ノード１００にグループ外のノード１００が利用可能なアプリケーションが実装されている場合、ノード１００に実装されている各アプリケーションに対するアクセス制御のために用いる情報が格納されているテーブルである。

【０１０６】

なお、本テーブルは、ノード１００がグループ内からのアクセスに対してのみ提供するアプリケーションだけを実装している場合は不要なものである。

【０１０７】

アクセス制御対象アプリケーション管理テーブル７００の一例を図９に示す。

【０１０８】

本図に示すように、アクセス制御対象アプリケーション管理テーブル７００は、グループ外のノード１００にも開放されているアプリケーションが利用するポート番号を格納するポート番号格納フィールド７０１（７０１Ａ、７０１Ｂ）を備える。各ノード１００は、ＩＰパケット受信時に、本テーブルを参照し、当該ＩＰパケットがアクセスしようとしているアプリケーションがグループ外のノード１００にも開放されたアプリケーションであるか否かの判定を行う。

【０１０９】

次に、グループメンバ管理テーブル８００について説明する。各ノード１００間で、ＩＰｖ６に基づき、ＩＰパケット通信を行なうためには、各ノード１００のＩＰアドレスを知る必要がある。グループに属する各ノード１００のＩＰアドレスは、グループ参加時に取得した各ノード１００のホスト名からＩＣＭＰ(Internet Control Message Protocol) Echo Request/Replyパケットのやりとりにより、アドレスの解決を行なうことで取得する。このように、グループメンバ管理テーブル８００は、各ノードにおいてホスト名からＩＰアドレスを解決して作成するもので、そこには、グループに属する各ノード１００のホスト名とＩＰアドレスとの対応が格納されている。

【０１１０】

図１０にグループメンバ管理テーブル８００の一例を示す。

【０１１１】

本図に示すように、本テーブルは、ノードを特定するホスト名を格納するホスト名格納フィールド８０１と、ホスト名と対応させて各ノード１００のＩＰアドレスを格納するＩＰアドレス格納フィールド８０２と、ＩＰアドレスの有効期限を格納する有効期限格納フィールド８０２とを備える。

【０１１２】

ノード１００が再起動した場合などに、ノード１００のＩＰアドレスは変わる可能性がある。また、一定時間内にＩＰアドレス格納部８０２に格納されているＩＰアドレスと送受信が行われないと、有効期限が切れる場合がある。

【０１１３】

このようなノードに対しＩＰパケットを送信する場合、ノード１００のＩＰｖ６送信前処理部３０５は、ＩＣＭＰ Echo Request/Replyパケットのやりとりにより、ホスト名からアドレスの解決を再度行ない、グループ管理処理部３０２に通知する。それを受けて、グループ管理処理部３０２のグループ情報更新処理部３５００は、ＩＰアドレスが登録されている本テーブルおよびグループ内の通信に利用するセキュリティアソシエーションを更新する。

【０１１４】

次に、ＳＡデータベース３０９に格納されている、セキュリティアソシエーション９００について説明する。セキュリティアソシエーション９００は、ＩＰｓｅｃにのっとった通信を行うために共有すべき情報を管理するものであり、例えば、ノード１００Ａとノード１００Ｂ間で通信する場合、ノード１００Ａからノード１００Ｂ方向の通信、および、ノード１００Ｂからノード１００Ａ方向の通信、両者に対し、独立して設定する必要があるものである。

【０１１５】

図１１に、セキュリティアソシエーション９００の一例を示す。

【０１１６】

本図に示すように、セキュリティアソシエーション９００は、各セキュリティアソシエーションを識別するＳＰＩ(セキュリティポリシ識別子)、送信元ＩＰアドレス、送信先アドレス、プロトコルとして認証あるいは暗号の指定、暗号範囲としてトランスポートモードあるいはトンネルモードの指定、暗号アルゴリズム、暗号鍵、認証アルゴリズム、認証鍵、鍵の有効期限などを含む。

【０１１７】

本実施形態では、各ノード１００においてセキュリティアソシエーション９００を作成するにあたり、送信用のセキュリティアソシエーション９００を作成する場合は、送信元ＩＰアドレスには、自身のノード１００のＩＰアドレスを、送信先ＩＰアドレスには、通信相手先ノードのＩＰアドレスを設定し、受信用を作成する場合は、送信元ＩＰアドレスには、通信相手先のＩＰアドレスを設定し、送信先ＩＰアドレスには、自身のノード１００のＩＰアドレスを設定する。

【０１１８】

ＳＰＩには、送信用、受信用ともに、グループ管理テーブル６００のグループ識別子格納部６０１に格納されているグループ識別子が格納される。また、送信用、受信用ともに、プロトコル、認証鍵アルゴリズム、認証鍵、有効期限には、それぞれ、グループ管理テーブル６００に格納されているものが設定される。

【０１１９】

以上、本実施形態におけるノード１００の各機能などについて説明した。

【０１２０】

次に、本実施形態における、ネットワーク１１０に接続された各ノード１００間で、グループを生成し、参加する手順、また、一旦参加したグループから離脱する手順などを説明する。

【０１２１】

以下においては、ＩＰｓｅｃの機能種別としてＡＨを、モードとしてトランスポートモードを、認証アルゴリズムとしてＳＨＡ－１（Secure Hash Algorithm 1:SHS(Secure Hash Standard) FIPS 180として規定）を用いる場合を例にあげ、説明する。ＩＰｓｅｃ通信の設定は、これらに限られない。

【０１２２】

また、本実施形態においては、前述したように、グループの情報を格納するメモリカードと、グループを離脱する際に用いる空のメモリカードとの２つのメモリカードを用いてグループの生成、参加、離脱、情報更新などを行なう。

【０１２３】

図１２に、グループ管理処理部３０２が行なうグループ管理処理手順３０２０を示す。

【０１２４】

グループ管理処理手順３０２０は、ユーザがメモリカードを各ノード１００の記録媒体インタフェース２０６に挿入することをきっかけに開始される。

【０１２５】

そして、ノード１００の記憶媒体インタフェース処理部３１８は、メモリカードが記録媒体インタフェース２０６に挿入されたことを検出すると、記憶媒体イ

ンタフェース２０６に備えられているＬＥＤライトを点灯し、メモリカードを利用中であることを利用者に対して示す。

【０１２６】

ＬＥＤライトが消灯されたことにより、ユーザは処理が終了したことを知り、メモリカードを取り出すことができる。

【０１２７】

また、記憶媒体インタフェース処理部３１８は、メモリカードを検出したことをグループ管理処理部３０２へ通知する。その通知を受けて、グループ管理処理部３０２は、グループ管理処理１０００を開始する。

【０１２８】

まず、グループ管理処理部３０２の制御部３１００は、自身のアクセスポリシデータベース３０８と、記録媒体インタフェース処理部３１８を介してメモリカード挿入されたメモリカードとにアクセスし、グループ管理テーブル６００の有無を確認する（ステップ３０２１）。

【０１２９】

ここで、どちらにもグループ管理テーブル６００がない場合、グループ自体が存在しない、すなわち、グループを生成する必要があると判断し、制御部３１００は、グループ生成処理部３２００にグループ生成処理３２１０を行わせる（ステップ３０２２）。グループ生成処理３２１０が完了すると、制御部３０２は、記憶媒体インタフェース処理部３１８に対し、メモリカードの書き込み終了を通知し（ステップ３０２７）、処理を終える。

自身のアクセスポリシデータベース３０２には無く、メモリカードには存在した場合、制御部３１００は、メモリカードに存在するグループに自身が参加しようとしていると判断し、グループ参加処理部３３００にグループ参加処理３３１０を行なわせ（ステップ３０２３）、グループ参加処理が完了すると、ステップ３０２７に進む。

【０１３０】

メモリカードには無く、自身のアクセスポリシデータベース３０２には存在した場合、制御部３１００は、自身は既にグループに属しているが空白のメモリカ

ードが挿入されたことにより、グループ離脱処理を行なうものと判断し、グループ離脱処理部３４００にグループ離脱処理３４１０を行なわせ（ステップ３０２６）、グループ離脱処理が完了するとステップ３０２７に進む。

【０１３１】

どちらにもグループ管理テーブル６００が存在する場合は、制御部３１００は、まず、アクセスポリシデータベース３０２内のグループ管理テーブル６００とメモリカード内のグループ管理テーブル６００とのグループ識別子を比較する（ステップ３０２４）。

【０１３２】

ここで、両者が同じであれば、メモリカードのグループ情報を更新する処理を行なうものと判断し、グループ情報更新処理部３５００にグループ情報更新処理３５１０としてアクセスポリシデータベース３０２内のグループ管理テーブル６００をメモリカードにコピーする処理を行なわせ（ステップ３０２５）、当該処理が完了すると、ステップ３０２７に進む。

【０１３３】

ステップ３０２４において、両者が異なった場合、制御部３１００は、誤ったメモリカードが挿入されたと判断し、そのままステップ３０２７にすすむ。

【０１３４】

次に、グループ生成処理１２００、グループ参加処理１３００、グループ離脱処理１６００、グループ情報更新処理１５００の手順を説明する。

【０１３５】

まず、グループ生成処理３２１０の処理手順を図１３に示す。

【０１３６】

制御部３１００から処理開始の指示を受けると、グループ生成処理部３２００は、グループ鍵を生成し（ステップ３２１１）、グループを識別するためのグループ識別子を生成し（ステップ３２１２）、認証・暗号モードとして認証（ＡＨ）を選択し（ステップ３２１３）、アルゴリズムとしてＳＨＡ－１を選択する（ステップ３２１４）。

【０１３７】

そして、それぞれを、グループ鍵格納フィールド６０２、グループ識別子格納フィールド６０１、ＩＰｓｅｃ種別格納フィールド６０４、アルゴリズム格納フィールド６０５に格納し、グループ管理テーブル６００を作成する（ステップ３２１５）。そして、ホスト名格納フィールド６０６に自ノード１００のホスト名を登録する（ステップ３２１６）。

【０１３８】

グループ管理テーブル６００が完成すると、グループ生成処理部３２００は、本テーブルをメモリカードにコピーすると共に、自ノード１００のアクセスポリシデータベース３０８に記憶し（ステップ３２１７，３２１８）、処理が終了したことを制御部３１００に通知する。

【０１３９】

次に、グループ参加処理３３１０の処理手順を図１４に示す。

【０１４０】

制御部３１００から処理開始の指示を受けると、グループ参加処理部３３００は、メモリカード上のグループ管理テーブル６００のホスト名格納フィールド６０６に自ノード１００のホスト名を追加し（ステップ３３１１）、メモリカード上のグループ管理テーブル６００を自身のアクセスポリシデータベース３０８内に記憶する（ステップ３３１２）。

【０１４１】

次に、グループメンバ管理テーブル８００を作成するとともに、グループに既に属している各ノード１００に、自身の参加を通知する新メンバ通知処理３７１０を行なう（ステップ３３１３）。

【０１４２】

そして、今までのステップで記録されたグループ管理テーブル６００の情報およびグループメンバ管理テーブル８００の情報とを用い、各ノード１００とのＩＰｓｅｃ通信に用いるセキュリティアソシエーション９００を生成し（ステップ３３１４）、処理が終了したことを制御部３１００に通知する。

【０１４３】

ここで、新メンバ通知処理３７１０についてその処理手順を説明する。図１５

にその処理手順を示す。

【０１４４】

新メンバ通知処理３７１０では、グループ管理テーブル６００内のホスト名フィールド６０６に格納されているホストごとに順に、ＩＣＭＰ Echo Request / ReplyによりＩＰアドレスを取得し（ステップ３７１２）、グループメンバ管理テーブル８００に、ホスト名ごとに取得したＩＰアドレスを登録する（ステップ３７１３）。

【０１４５】

上記のステップで取得した、グループを構成する各ノード１００のＩＰアドレスに対して加入コマンドを生成し（ステップ３７１４）、それを送信する（ステップ３７１５）。

【０１４６】

そして、次のホスト名を読み出して、ステップ１３３０から１３６０の処理を繰り返す（ステップ３３１６）。ここで、読み出したホスト名が自身のホスト名の場合は、何も処理を行わず、次のホスト名を読み出す（ステップ３７１１）。そして、グループ管理テーブル６００のホスト名格納フィールド６０６に格納されている、自身のノード１００を除く全てのノードに対して以上の処理を終えると（ステップ３７１７）、グループ内への新メンバ通知処理１３３０を終える。

【０１４７】

以上、グループ参加処理３３１０について説明した。

【０１４８】

次に、グループ離脱処理３４１０について、図１６を用いて説明する。

【０１４９】

制御部３１００から処理開始の指示を受けると、グループ離脱処理部３４００は、ノード１００内のグループ管理テーブル６００のホスト名格納部６０６に登録されているホスト名を順番に読み出す（ステップ３３１１）。

【０１５０】

ここで、読み出したホスト名が自ホスト名と一致した場合は、次のホスト名を読み出す。

【０１５１】

読み出したホスト名が自ホスト名と一致しない場合は、グループメンバ管理テーブル８００から読み出したホスト名に対応するＩＰアドレスを検索する（ステップ３３１２）。以後、このＩＰアドレスを検索したＩＰアドレスと呼ぶ。

【０１５２】

次に、送信先ＩＰアドレスを検索したＩＰアドレスとした離脱コマンドを作成し（ステップ３３１３）、その送信先ＩＰアドレスを有するノード１００に送信する（ステップ３３１４）。

【０１５３】

グループ離脱処理部３４００は、自身の保有するグループメンバ管理テーブル８００から以上の操作を行なった検索したＩＰアドレスに係わるデータを削除する（ステップ３３１５）。

【０１５４】

次に、ＳＡデータベース３０９に記憶されているセキュリティアソシエーション９００から検索したＩＰアドレスと等しい送信先ＩＰアドレスを持つものを抽出し、そのセキュリティアソシエーション９００を削除する（ステップ３３１６）。

【０１５５】

また、検索したＩＰアドレスと等しい送信元ＩＰアドレスを持つセキュリティアソシエーション９００を抽出し、それを削除する（ステップ３３１７）。

【０１５６】

グループ離脱処理部３４００は、グループ管理テーブル６００に登録されている全てのホスト名に対して、以上のステップ３３１１～ステップ３３１７の処理を実行した後（ステップ３３１８）、自身が保有するグループ管理テーブル６００を削除し（ステップ３３１９）、グループ離脱処理３３１０を終了する。そして、制御部３１００に処理終了を通知する。

【０１５７】

次に、上記のグループ参加処理３３１０内のグループ内への新メンバ通知処理３７１０のステップ３７１５およびグループ離脱処理３３１０のステップ３３１

４において送信された、それぞれ加入コマンドおよび離脱コマンドを受信した場合の各ノード１００側での処理を以下に説明する。

【０１５８】

本処理は、グループ制御ＩＰパケット受信処理部３６００によって行なわれ、グループ制御ＩＰパケット受信処理３６１０と呼ぶ。図１７に本処理の手順を示す。

【０１５９】

グループを構成する各ノード１００は、ネットワークインタフェース受信処理部３１０においてグループ制御ＩＰパケットを受信すると、ＩＰ受信部３１４、ＴＣＰ／ＵＤＰ受信処理部３１５を経てグループ管理処理部３０２のグループ制御ＩＰパケット受信処理部３６００へ受け渡す。

【０１６０】

受信したグループ制御ＩＰパケット受信処理部３６００は、コマンド識別子格納部１００１に設定されているコマンド識別子が加入であるか否かを確認する（ステップ３６１１）。

【０１６１】

ステップ３６１１でコマンド識別子が加入を示す（００）hexであった場合、すなわち、加入コマンドを受信した場合、ステップ３６１２に進み、グループ制御ＩＰパケットのホスト名１００３に設定されている加入コマンドを送信してきたノード１００のホスト名をグループ管理テーブル６００に登録する（ステップ３６１２）。

【０１６２】

そして、グループメンバ管理テーブル８００に、加入コマンドを送信してきたノード１００のホスト名と、グループ制御ＩＰパケットのＩＰアドレス格納部１００２に設定されているそのＩＰアドレスとを登録する（ステップ３６１３）。

【０１６３】

次に、グループ制御ＩＰパケット受信処理部３６００は、送信用、すなわち、自身のノード１００から加入コマンドを送信してきた新規に加入したノード１００方向の送信、および、受信用、すなわち、加入コマンドを送信してきた新規に

加入したノード１００から自身のノード１００方向の送信、各々のセキュリティアソシエーション９００を作成する処理を行なう（ステップ３６１４、３６１５）。

【０１６４】

次に、ステップ３６１１でコマンド識別子が離脱を示す（０１）hexであった場合、すなわち、離脱コマンドを受信した場合、グループ制御ＩＰパケット受信処理部３６００は、ステップ３６１６に進む。

【０１６５】

ここで、グループ制御ＩＰパケット受信処理部３６００は、ＳＡデータベース３０９に記憶されているセキュリティアソシエーション９００から、受信したグループ離脱コマンドのデータ部１０００のＩＰアドレス１００２に格納されているＩＰアドレスと等しい送信先ＩＰアドレスを持つものを抽出し、抽出したセキュリティアソシエーションを削除する（ステップ３６１６）。

【０１６６】

次に、受信した離脱コマンドのＩＰアドレス１００２と等しいＩＰアドレスを有するデータをグループメンバ管理テーブル８００から削除し（ステップ３６１７）、受信した離脱コマンドのホスト名１００３に格納されているホスト名と等しいホスト名を、自ノード１００上のグループ管理テーブル６００から削除する（ステップ３６１８）。

【０１６７】

グループ内の全てのノード１００において以上の手順を行なうことにより、全てのノード１００が保有する離脱したノード１００に対応するセキュリティアソシエーション９００を削除し、また、グループ管理テーブル６００から、離脱したノード１００の情報を削除する。

【０１６８】

以上のようにして、グループを構成するノード１００に新規加入または離脱といった変更があった場合、当該ノード１００から送信されるグループ制御ＩＰパケットを受信した他のノード１００において、自身の保有するセキュリティアソシエーションおよびグループ管理テーブル６００が更新される。

【０１６９】

以上、グループ制御ＩＰパケット受信処理を説明した。

【０１７０】

ここまで、グループ管理処理部３０２による、グループの生成、参加、離脱などのグループ管理処理について説明した。

【０１７１】

次に、上記の手順で生成され管理されているグループ内で、アプリケーションを互いに利用する手順を以下に説明する。

【０１７２】

アプリケーションの利用は、ＩＰパケットを互いに送受することによって行なわれる。まず、このＩＰパケットの送受信について説明する。

【０１７３】

前述のように、ＩＰｓｅｃ通信を行うために予め設定の必要なセキュリティアソシエーション９００は、グループ管理処理３０２において、新たなグループ構成メンバが追加される際に生成される。すなわち、グループに属している限り、ＩＰｓｅｃ通信は可能である。

【０１７４】

ＩＰパケットを送信するにあたり、ＩＰｓｅｃ送信処理部３０６は、送信するＩＰヘッダの送信先ＩＰアドレスをキーに、ＳＡデータベース３０９を検索し、対応するＩＰアドレスが送信先ＩＰアドレスとして格納されているセキュリティアソシエーション９００を抽出する。抽出したセキュリティアソシエーション９００に登録されている情報に基づき、ＩＰｓｅｃ処理を行い、ＩＰｖ６送信後処理３０７を行い、ネットワークインタフェース送信処理部を介して、送信先ノードにＩＰパケットを送信する。

【０１７５】

次に、ＩＰパケット受信時の処理手順を図１８を用いて説明する。

【０１７６】

ネットワークインタフェース受信処理部３１０を介してＩＰパケットを受信すると、ＩＰｖ６受信前処理部３１１は、ＩＰｖ６受信前処理を行い（ステップ４

０１０）、受信したＩＰヘッダ内の、ＡＨヘッダの有無をチェックする（ステップ４０２０）。

【０１７７】

受信したＩＰヘッダ内にＡＨヘッダ４０１があると判断したならば、そのＩＰパケットをＩＰｓｅｃ受信処理部３１２に受け渡す。

【０１７８】

受け取ったＩＰｓｅｃ受信処理部３１２は、後述するＩＰｓｅｃ受信処理３１２０を行い（ステップ４０３０）、ＩＰｖ６受信後処理部３１３にＩＰパケットを受け渡す。

【０１７９】

そして、ＩＰｖ６受信後処理部３１３は、ＩＰｖ６受信後処理３１３０を行い（ステップ４０４０）、処理を終了する。

【０１８０】

なお、ここで、ＩＰｖ６受信後処理部３１３は、ＩＰｖ６受信後処理３１３０を終えた受信したパケットをＴＣＰ/ＵＤＰ受信処理部３１５に受け渡す。受け取ったＴＣＰ/ＵＤＰ受信処理部３１５は、受け取ったパケットの受信処理を行い、アプリケーション３０１に受信データとして渡す。

【０１８１】

ステップ４０２０で、上記のヘッダがないと判断した場合、そのＩＰパケットを受信アクセス制御部３１６に受け渡す。

【０１８２】

受け取った受信アクセス制御部３１６は、それがＩＣＭＰパケットであるか否かチェックする（ステップ４０５０）。

【０１８３】

ステップ４０５０で、受信したＩＰパケットが、ＩＣＭＰパケットであると判断されたならば、そのままＩＰｖ６受信後処理部３１３に受け渡し、ＩＰｖ６受信後処理３１３０を行い（ステップ４０４０）、処理を終了する。

【０１８４】

ステップ４０５０で、ＩＣＭＰパケットではないと判断されたならば、受信ア

クセス制御部３１６は、そのＩＰパケットをグループ外のノード１００から送信されたグループ外ＩＰパケットであると判断し、後述するグループ外ＩＰパケット受信処理３１６０を行い（ステップ４０６０）、処理を終了する。

【０１８５】

次に、上記のＩＰｓｅｃ処理３１２０について説明する。

【０１８６】

ＩＰｓｅｃ処理部３１２は、ＡＨヘッダを有するＩＰパケットを受信すると、ＩＰヘッダの送信元ＩＰアドレス、送信先ＩＰアドレス、ＡＨヘッダ４０１に設定されているＳＰＩが一致するセキュリティアソシエーション９００をＳＡデータベース３０９から抽出する。

【０１８７】

そして、抽出したセキュリティアソシエーション９００に記憶されている認証鍵を用いて受信したＩＰパケットの認証情報を作成し、ＡＨヘッダ４０１に設定されている認証情報と比較する。

【０１８８】

両者が一致していれば、受信したＩＰパケットをグループに属する正当なノード１００からの送信とみなし、ＩＰｖ６受信後処理部３１３に受け渡す。そして、一致しない場合は、そのＩＰパケット破棄する。

【０１８９】

以上ＩＰｓｅｃ処理３１２０について説明した。

【０１９０】

次に、受信アクセス制御部３１６によるグループ外パケット受信処理３１６０について説明する。

【０１９１】

以上のように、本実施形態においては、グループに属するノード１００は、グループ外のノード１００から、ＡＨヘッダを有するＩＰパケットを受信した場合は、ＩＰｓｅｃ通信処理部３１２において、また、ＡＨヘッダを有しないＩＰパケットを受信した場合は、ＩＰｖ６受信前処理部３１１において、当該ＩＰパケットが、ＩＰｖ６受信後処理部３１３、ＴＣＰ/ＵＤＰ受信処理部３１５を介し

てアプリケーション３０１に到達することを排除している。

【０１９２】

しかし、本実施形態においては、ノード１００によっては、その保有するアプリケーションの利用を、グループ外のノード１００にも開放しているものがある。前述したように、このようなアプリケーションを有するノード１００は、アプリケーションごとのポート番号を、アクセス制御対象アプリケーション管理テーブル７００において管理している。

【０１９３】

グループ外のノード１００からＡＨヘッダを有するＩＰパケットを受信した場合は、そのＩＰパケットを復号することができないため、それはＩＰｓｅｃ通信処理部３１２において破棄することは先に説明した。

【０１９４】

グループ外ＩＰパケット受信処理３１６０は、グループ外のノード１００から通常のＩＰパケットを受信した際に、グループ外のノード１００に開放しているアプリケーションに当該ＩＰパケットを送達する処理である。

【０１９５】

グループ外ＩＰパケット受信処理３１６０では、ＩＰパケットを受け取ったノード１００が、グループ外のノード１００に対し何らサービス機能を提供しない場合、アクセスエラーをデータとして格納したＩＰパケットを送信元に対して送信し、受信したＩＰパケットは破棄する。これに対し、グループ外のノード１００に対して何らかのサービス機能を提供する場合は、アクセス制御対象アプリケーション管理テーブル７００の登録に従って、アプリケーションを提供するよう制御している。

【０１９６】

以下にその手順を図１９を用いて説明する。

【０１９７】

受信アクセス制御部３１６は、ＩＰｖ６受信前処理部３１１からＩＣＭＰパケットではないＩＰパケットを受信した場合、当該ＩＰパケットから読取った送信先ポート番号とアクセス制御対象アプリケーション管理テーブル７００に登録さ

れているポート番号７０１との比較を行なう（ステップ３１６１）。

【０１９８】

アクセス制御対象アプリケーション管理テーブル７００には、グループ外のノードに利用が許可されているアプリケーションのポート番号が登録されているため、両者が一致した場合、サービス機能を要求元ノード１００に提供できることとなる。

【０１９９】

この場合、受信アクセス制御部３１６は、受け取ったＩＰパケットをＩＰｖ６受信後処理部３１３に受け渡し、受け取ったＩＰｖ６受信後処理部３１３は、ＩＰｖ６受信後処理３１３０を行なう（ステップ３１６４）。

【０２００】

そして、ＩＰｖ６受信後処理部３１３から処理されたＩＰパケットを受け取ったＴＣＰ/ＵＤＰ受信処理部３１５は、それを、アプリケーション３０１に受け渡す。

【０２０１】

ステップ３１６１において、ポート番号が一致しない場合は、提供できるサービス機能がないため、受信アクセス制御部３１６は、アクセスエラーをデータとして格納したＩＰパケットを生成しＩＰ送信部３０４から送信元に送信し（ステップ３１６２）、受信したＩＰパケットは破棄する（ステップ３１６３）。

【０２０２】

以上、グループ外ＩＰパケット受信処理について説明した。

【０２０３】

このように、本実施形態においては、グループ内のノード１００間ではＩＰｓｅｃ通信を行い、グループ外のノード１００とは通常のＩＰパケットによる通信を行うことで、アクセス制御対象アプリケーション管理テーブル７００で管理している各アプリケーションのポート番号に従って、アプリケーションごとにグループ内外のアクセス許可を制御することができる。これにより、一つのノード１００において、グループだけで利用するサービス機能と、誰もが利用できるサービス機能とを実装し、それぞれへのアクセス制御を可能としている。

【０２０４】

本実施形態によれば、ホームネットワークを構成するノード１００において作成したグループ鍵を含むＩＰｓｅｃ通信に必要な情報を、共通のメモリカードを介して、利用者が相互に利用することを許可する各ノード１００に配布する。

【０２０５】

配布されたノード１００は、グループに所属している他のノード１００とＩＰｓｅｃ通信ができるように、セキュリティアソシエーション９００を設定するとともに、新規加入したことを、グループに所属している他のノード１００に通知する。

【０２０６】

通知を受けたノード１００は、それぞれ、新規に加入したノード１００とのＩＰｓｅｃ通信ができるように、セキュリティアソシエーション９００を設定する。

【０２０７】

以上のように、本実施形態では、例えば、通信を開始する際に認証サーバ、あるいは鍵管理手段を備えた装置等といったグループを構成する機器以外の装置を介さずに、互いに認証可能で安全な通信を行なうことのできるグループを、そのグループを構成する機器が、容易に生成し管理することを実現している。

【０２０８】

また、グループを生成し管理するために必要な情報を、メモリカードといった記憶媒体を介して各ノードに与えること、および、グループの生成、グループへの参加、および、グループからの離脱の指示を各ノードに与えることを実現している。

【０２０９】

このように、本実施形態では、サーバなどの特別な機器を設けることなく、また、複数のマスタ鍵などを備えたＩＣカードを用意してグループを構成する機器それぞれに予めセットしておくなどの事前の準備をすることなく、グループを構成する機器間でのみ、容易にＩＰｓｅｃ通信可能な環境を構築できる。

【０２１０】

また、本実施形態では、一つのノードに、グループ内のノードのみ利用できるアプリケーションとグループ外のノードも利用できるアプリケーションとが実装されている場合も容易にそれぞれのアクセス制御を実現できる。

【０２１１】

なお、本実施形態では、グループ生成、加入、離脱時の指示を行なう際に利用する記憶媒体としてメモリカードを例にあげ、説明したが、利用する記憶媒体はこれに限られない。可搬型の記憶媒体であり、各ノードがそのインタフェースを備えていれば、どのような記憶媒体であってもよい。

【０２１２】

また、本実施形態では、ＩＰｓｅｃ通信を行うために必要な情報の授受を記憶媒体で行なうといった設定としたが、これに限られない。例えば、各ノードに入力装置を備え、ユーザが入力するようにしてもよい。

【０２１３】

さらに、グループからの離脱処理を開始するきっかけとして、空のメモリカードの入力を例にあげ説明したが、これに限られない。例えば、各ノードがリセットボタンを備え、ユーザがそのリセットボタンを介して離脱処理を開始する指示を与えるようにしてもよい。

【０２１４】

また、ＬＥＤを備えることにより、利用者に対しグループ生成、加入処理の終了を通知する事を実現している。通知のための機能も、これに限られない。

【０２１５】

なお、本発明は上記の実施形態に限定されるものではなく、その要旨の範囲内で様々な変形が可能である。

【０２１６】

例えば、上記の実施形態では、宅内のネットワークを例にとり説明したが、本発明はこれに限定されない。本発明は、互いに認証を必要とする様々なネットワークシステムに広く適用できる。

【０２１７】

【発明の効果】

本実施形態においては、特別に認証サーバまたは鍵管理手段を備えた装置を保有しなくても、グループを構成する機器間で、互いにグループ構成機器であることを認証し、安全な通信を実現するグループを容易に生成し、管理することができる。

【０２１８】

また、機器がグループ内の機器にのみ提供するアプリケーションとグループ外の機器に提供するアプリケーションとを有する場合、そのアクセス制御を簡単な構成にて行なうことができる。

【図面の簡単な説明】

【図１】本発明を適用した実施形態のシステム構成を示す図である

【図２】本実施形態におけるノードのハードウェア構成を示す図である。

【図３】本実施形態におけるノードにおけるソフトウェア構成を示す図である。

【図４】グループ通信に用いるＡＨヘッダ付きのＩＰパケットの構成を示す図である。

【図５】グループ通信に用いるＥＳＰヘッダ付きのＩＰパケットの構成を示す図である。

【図６】本実施形態のおけるグループ管理処理部の機能構成を示す図である。

【図７】本実施形態におけるグループ制御ＩＰパケットのデータ部の構成の一例を示す図である。

【図８】グループ管理テーブルの構成の一例を示す図である。

【図９】アクセス制御対象アプリケーション管理テーブルの構成の一例を示す図である。

【図１０】グループメンバ管理テーブルの構成の一例を示す図である。

【図１１】セキュリティアソシエーションとして設定する情報構成の一例を示す図である。

【図１２】グループ管理処理の処理手順を示す図である。

【図１３】グループ生成処理の処理手順を示す図である。

【図１４】グループ参加処理の処理手順を示す図である。

【図１５】グループ内への新メンバ通知処理の処理手順を示す図である。

【図１６】グループ離脱処理の処理手順を示す図である。

【図１７】グループ制御ＩＰパケット受信処理の処理手順を示す図である。

【図１８】ＩＰパケット受信時のＩＰ受信部の処理手順を示す図である。

【図１９】ＩＰパケット受信時の受信アクセス制御部の処理手順を示す図である。

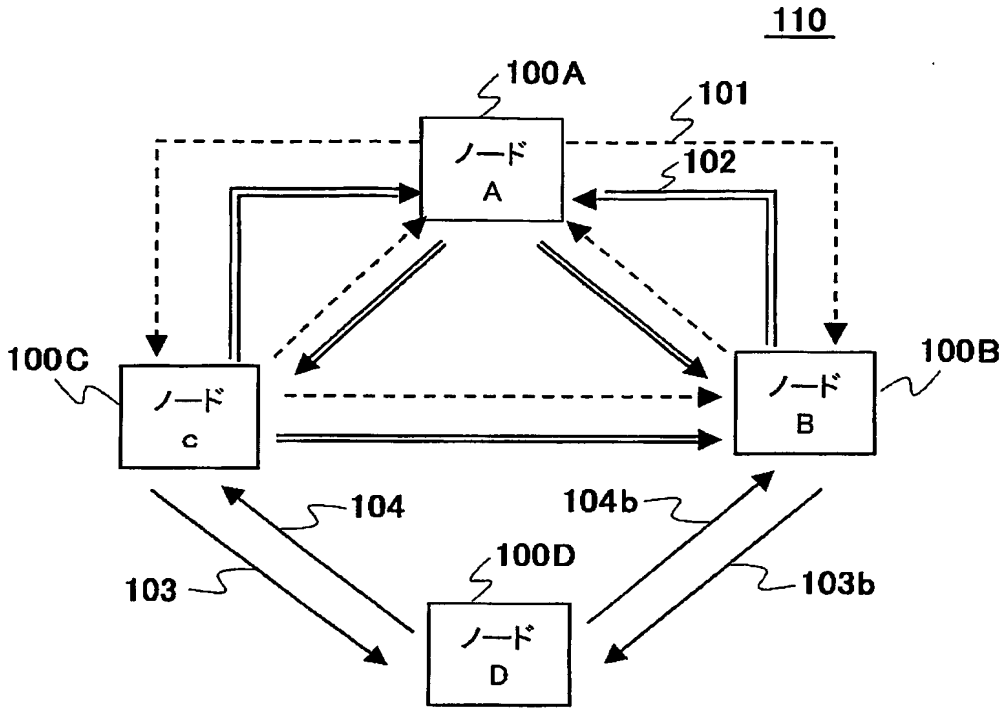
【符号の説明】

１００…ノード、３０１…アプリケーション、３０２…グループ管理処理部、３０８…アクセスポリシデータベース、３０９…ＳＡデータベース、３１４…ＩＰ受信部、３０４…ＩＰ送信部、３１２…ＩＰｓｅｃ受信処理部、３１６…受信アクセス制御部、６００…グループ管理テーブル、７００…アクセス制御対象アプリケーション管理テーブル、８００…グループメンバ管理テーブル、９００…セキュリティアソシエーション、３１００…制御部、３２００… グループ生成処理部、３３００…グループ参加処理部、３４００…グループ離脱処理部、３５００…グループ情報更新処理部、３６００…グループ制御ＩＰパケット受信処理部

【書類名】　図面

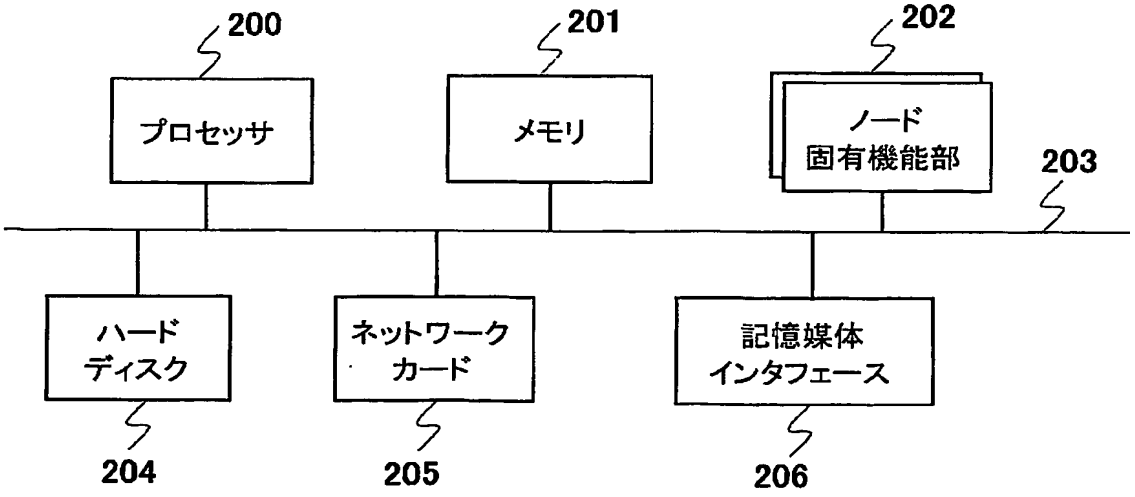
【図１】

図1



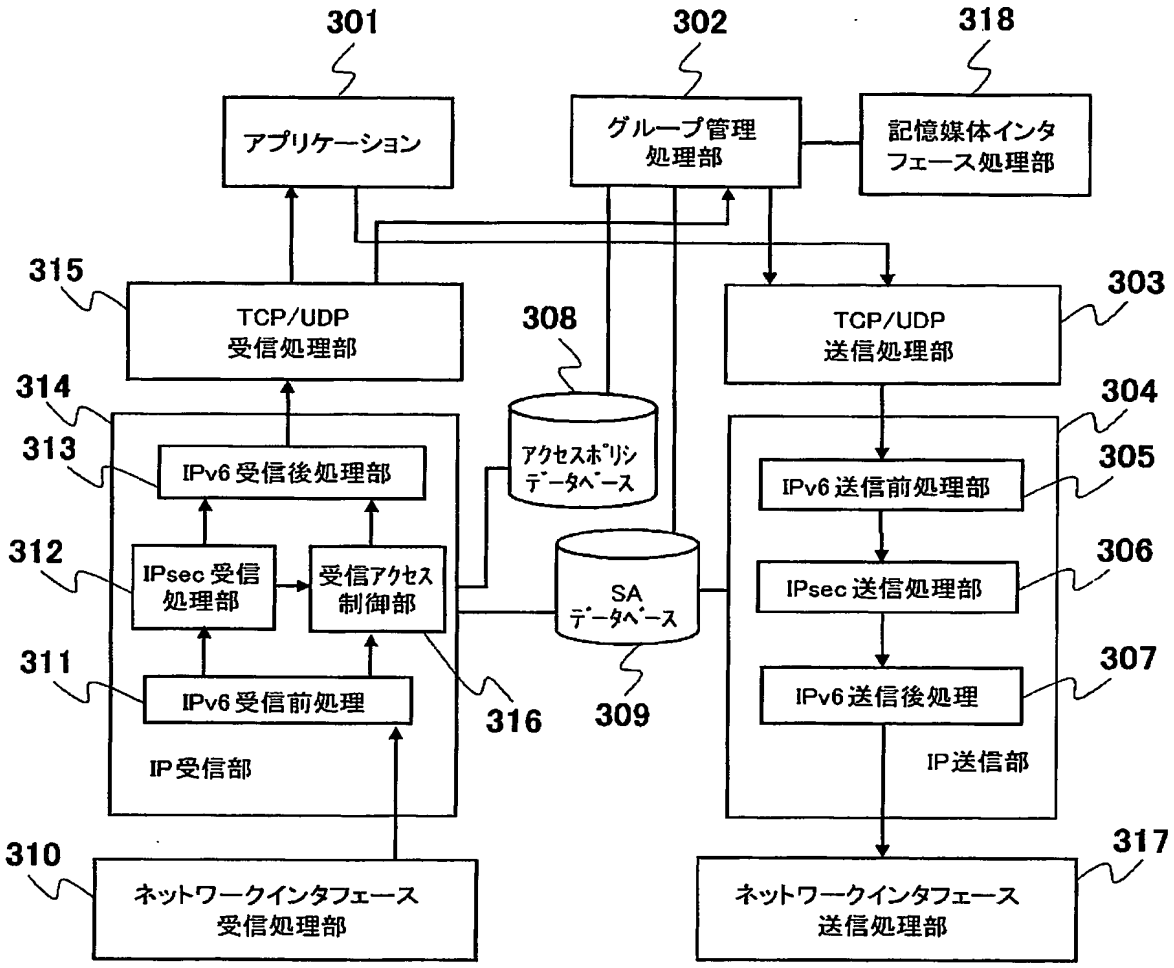
【図２】

図2



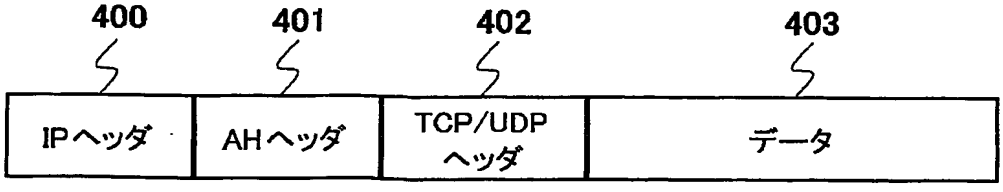
【図３】

図3


301
302
318
アプリケーション
グループ管理処理部
記憶媒体インタフェース処理部
315
TCP/UDP受信処理部
308
TCP/UDP送信処理部
303
314
304
313
IPv6受信後処理部
アクセスポリシデータベース
IPv6送信前処理部
305
312
IPsec受信処理部
受信アクセス制御部
SAデータベース
IPsec送信処理部
306
311
IPv6受信前処理
316
309
IPv6送信後処理
307
IP受信部
IP送信部
310
ネットワークインタフェース受信処理部
ネットワークインタフェース送信処理部
317

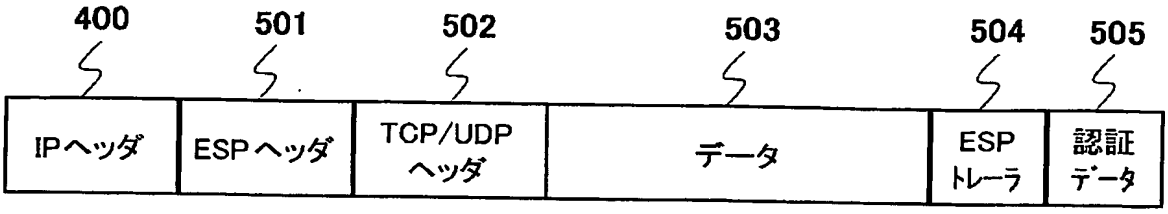
【図４】

図4


400
401
402
403
IPヘッダ
AHヘッダ
TCP/UDPヘッダ
データ

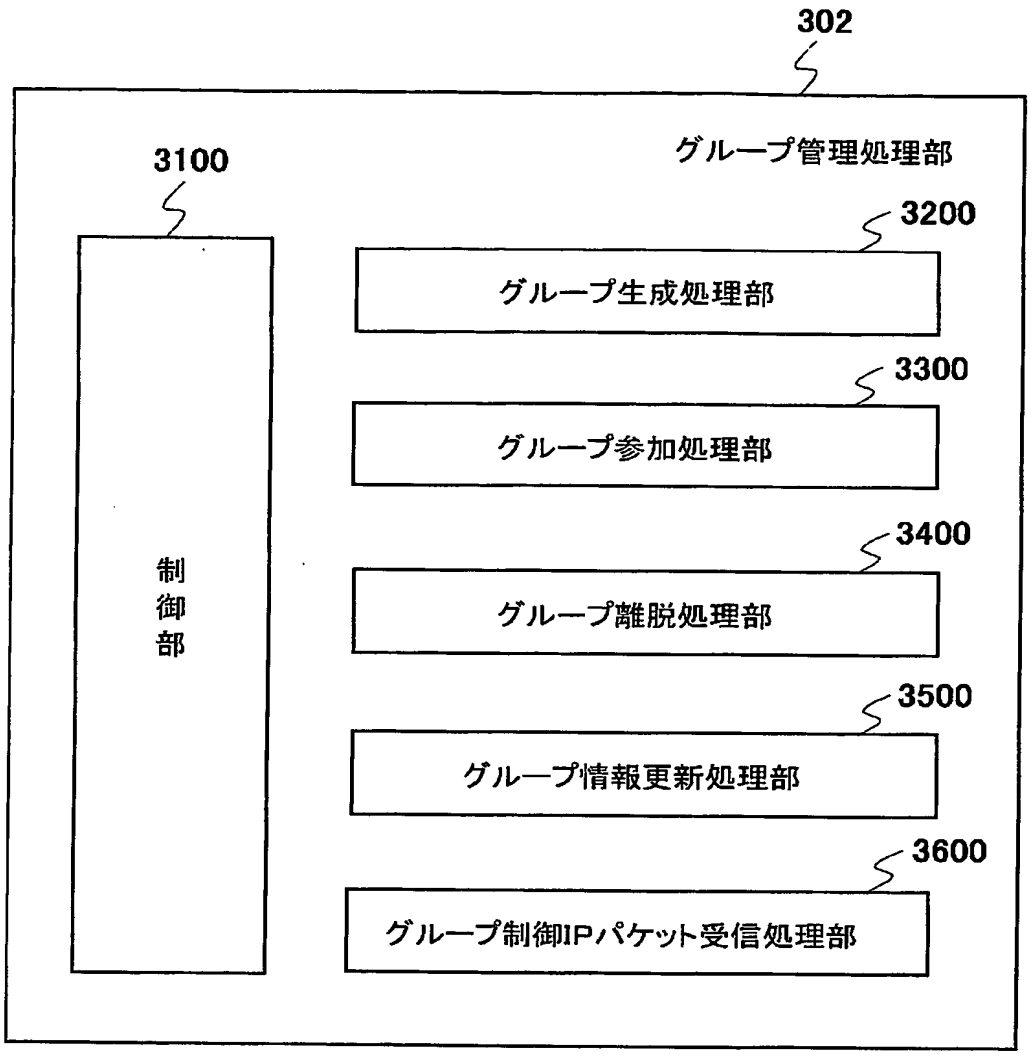
【図５】

図5


400
501
502
503
504
505
IPヘッダ
ESPヘッダ
TCP/UDP ヘッダ
データ
ESP トレーラ
認証 データ

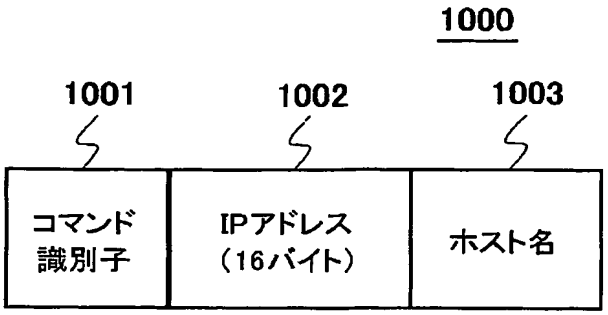
【図６】

図6


302
グループ管理処理部
3100
制御部
3200
グループ生成処理部
3300
グループ参加処理部
3400
グループ離脱処理部
3500
グループ情報更新処理部
3600
グループ制御IPパケット受信処理部

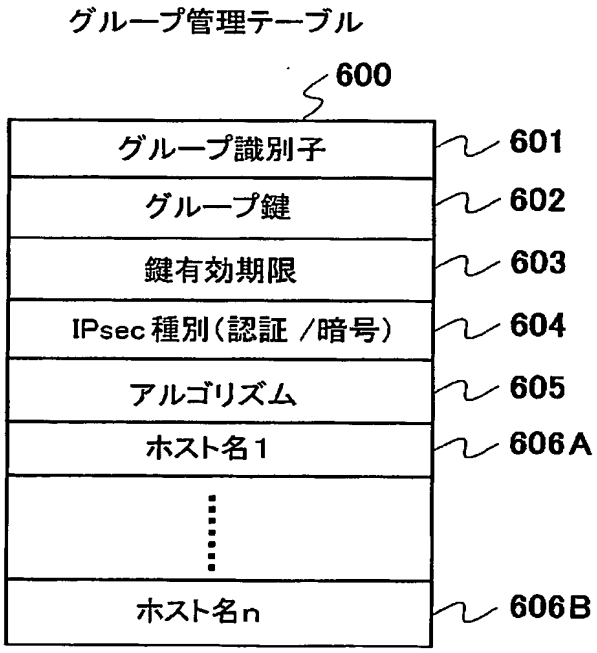
【図７】

図7


1000
1001
1002
1003
コマンド識別子
IPアドレス（16バイト）
ホスト名

【図８】

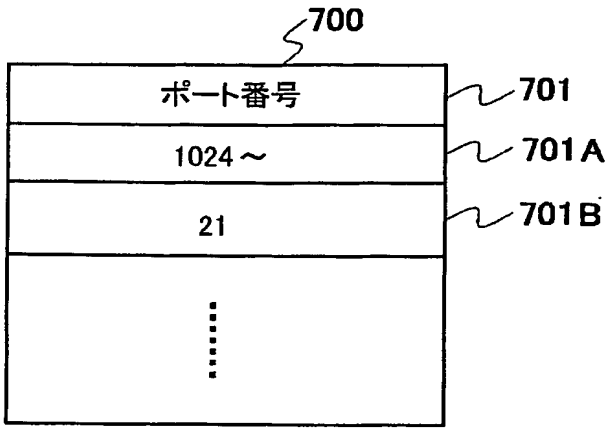
図8


グループ管理テーブル
600
グループ識別子
601
グループ鍵
602
鍵有効期限
603
IPsec種別（認証／暗号）
604
アルゴリズム
605
ホスト名1
606A
ホスト名n
606B

【図９】

図9

アクセス制御対象アプリケーション管理テーブル



【図１０】

図10

グループメンバ管理テーブル　800

801	802	803
ホスト名	IPアドレス	有効期限
ノードA	FE 80 :: 68 12 54 FE 35 01	××××
⋮	⋮	⋮

【図１１】

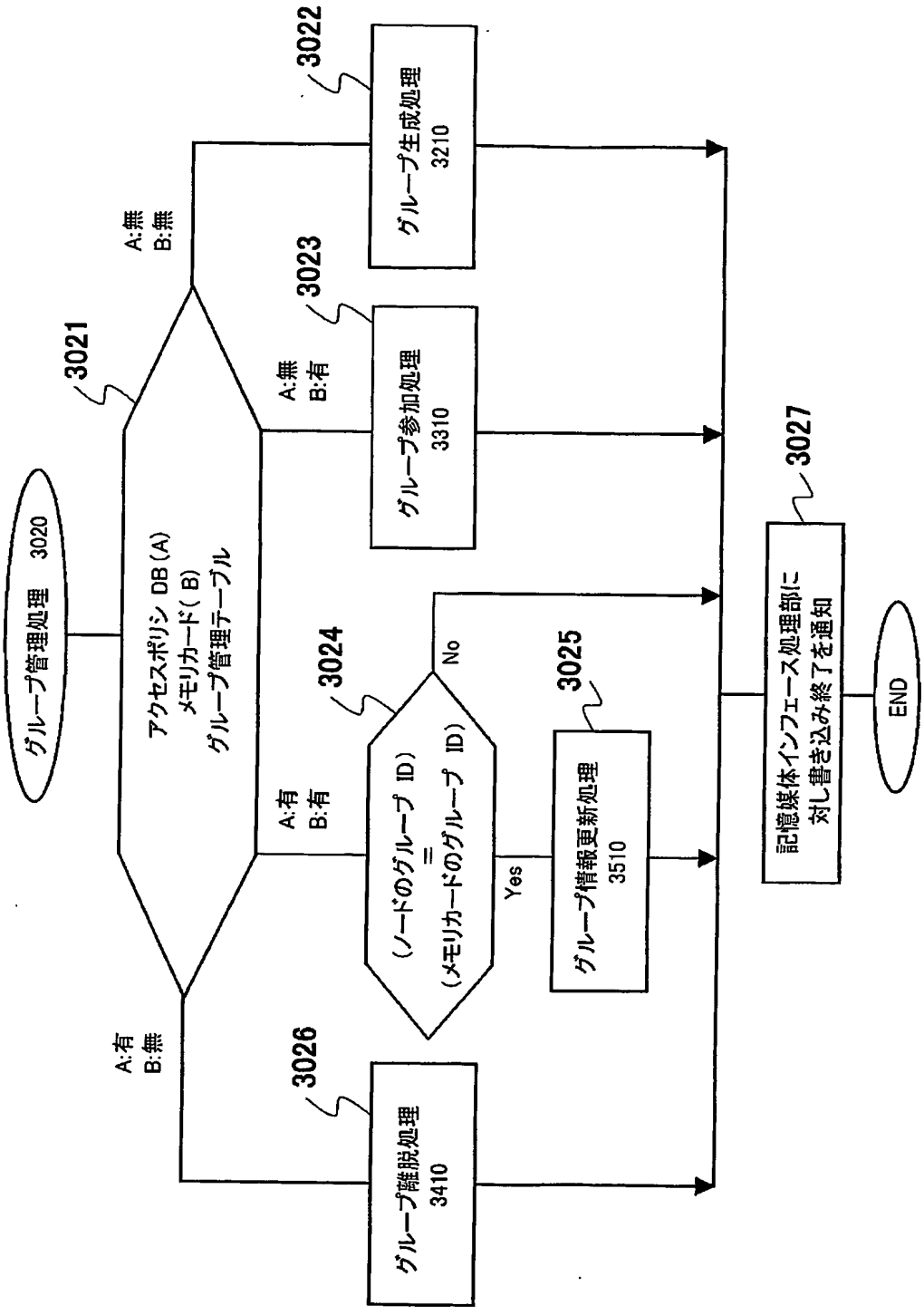
図11

セキュリティアソシエーション　900

SPI	グループ識別子
送信元IPアドレス	FE 80 :: 68 12 54 FE 35 01
送信先IPアドレス	FE 80 :: 68 12 54 FE 35 02
プロトコル	AH
モード	トランスポート
暗号アルゴリズム	――
暗号鍵	――
認証アルゴリズム	SHA-1
認証鍵	グループ管理テーブル上のグループ鍵
有効期限	in 7 days

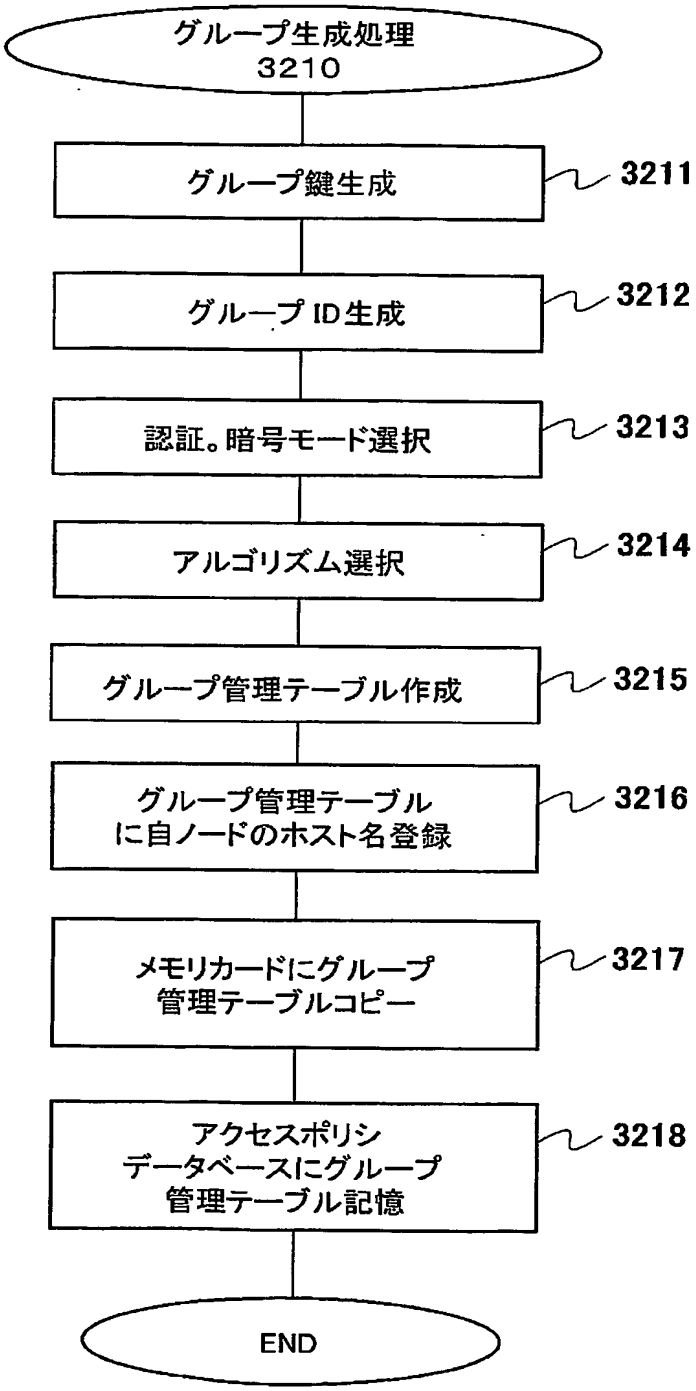
【図１２】

図12


グループ管理処理　3020
アクセスポリシ DB (A)
メモリカード(B)
グループ管理テーブル
3021
A:無
B:無
3022
グループ生成処理
3210
A:無
B:有
3023
グループ参加処理
3310
A:有
B:有
3024
(ノードのグループ ID)
=
(メモリカードのグループ ID)
No
Yes
3025
グループ情報更新処理
3510
A:有
B:無
3026
グループ離脱処理
3410
3027
記憶媒体インフェース処理部に
対し書き込み終了を通知
END

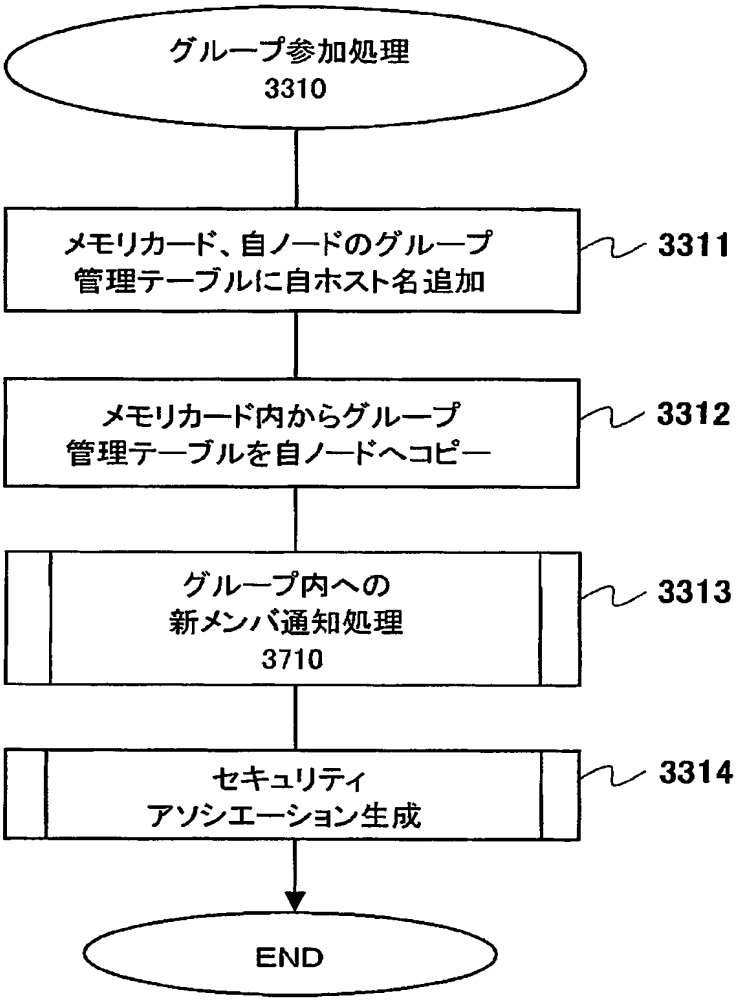
【図１３】

図13


グループ生成処理
3210
グループ鍵生成
3211
グループID生成
3212
認証。暗号モード選択
3213
アルゴリズム選択
3214
グループ管理テーブル作成
3215
グループ管理テーブル
に自ノードのホスト名登録
3216
メモリカードにグループ
管理テーブルコピー
3217
アクセスポリシ
データベースにグループ
管理テーブル記憶
3218
END

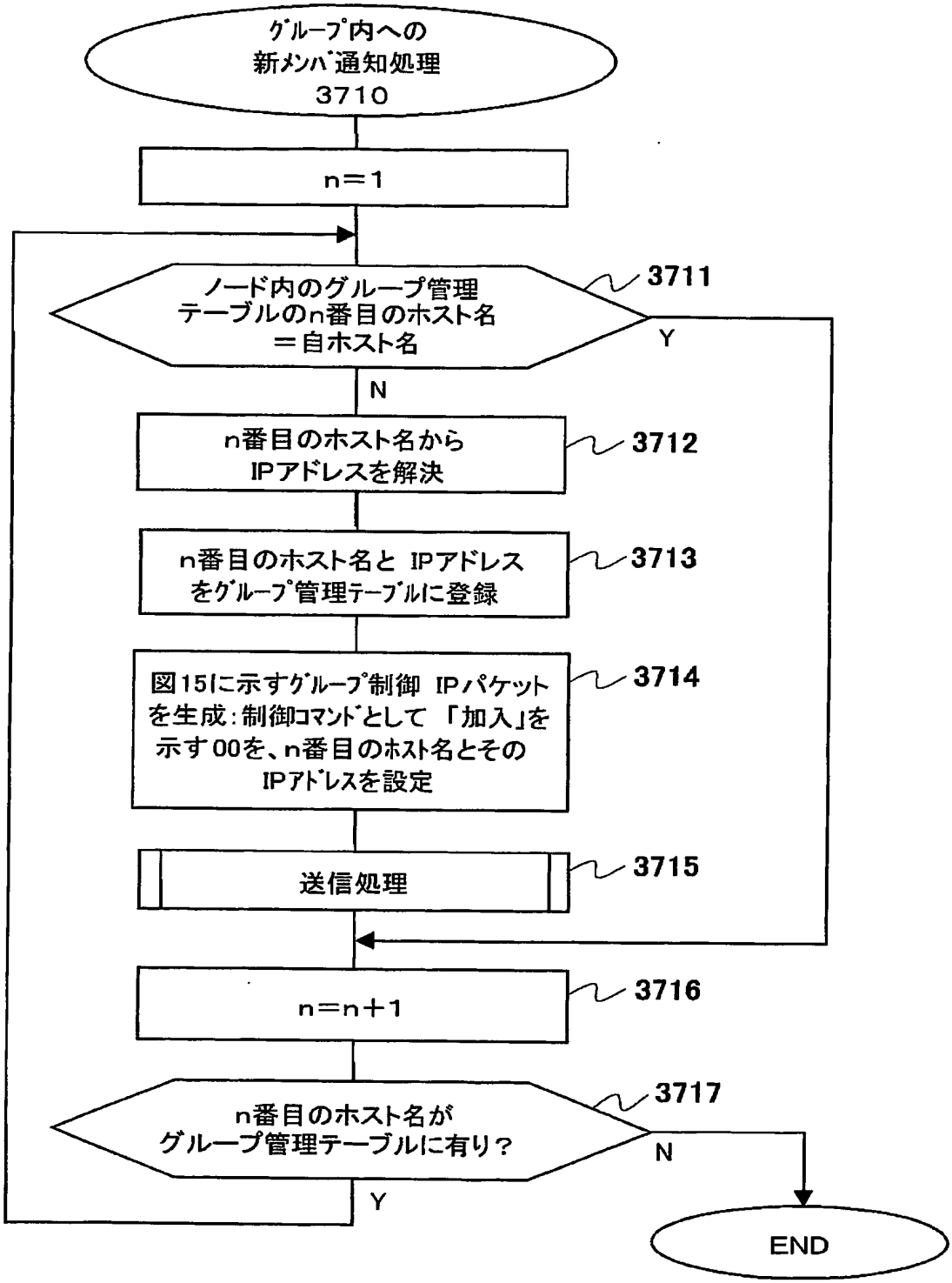
【図１４】

図14


グループ参加処理
3310
メモリカード、自ノードのグループ
管理テーブルに自ホスト名追加
3311
メモリカード内からグループ
管理テーブルを自ノードへコピー
3312
グループ内への
新メンバ通知処理
3710
3313
セキュリティ
アソシエーション生成
3314
END

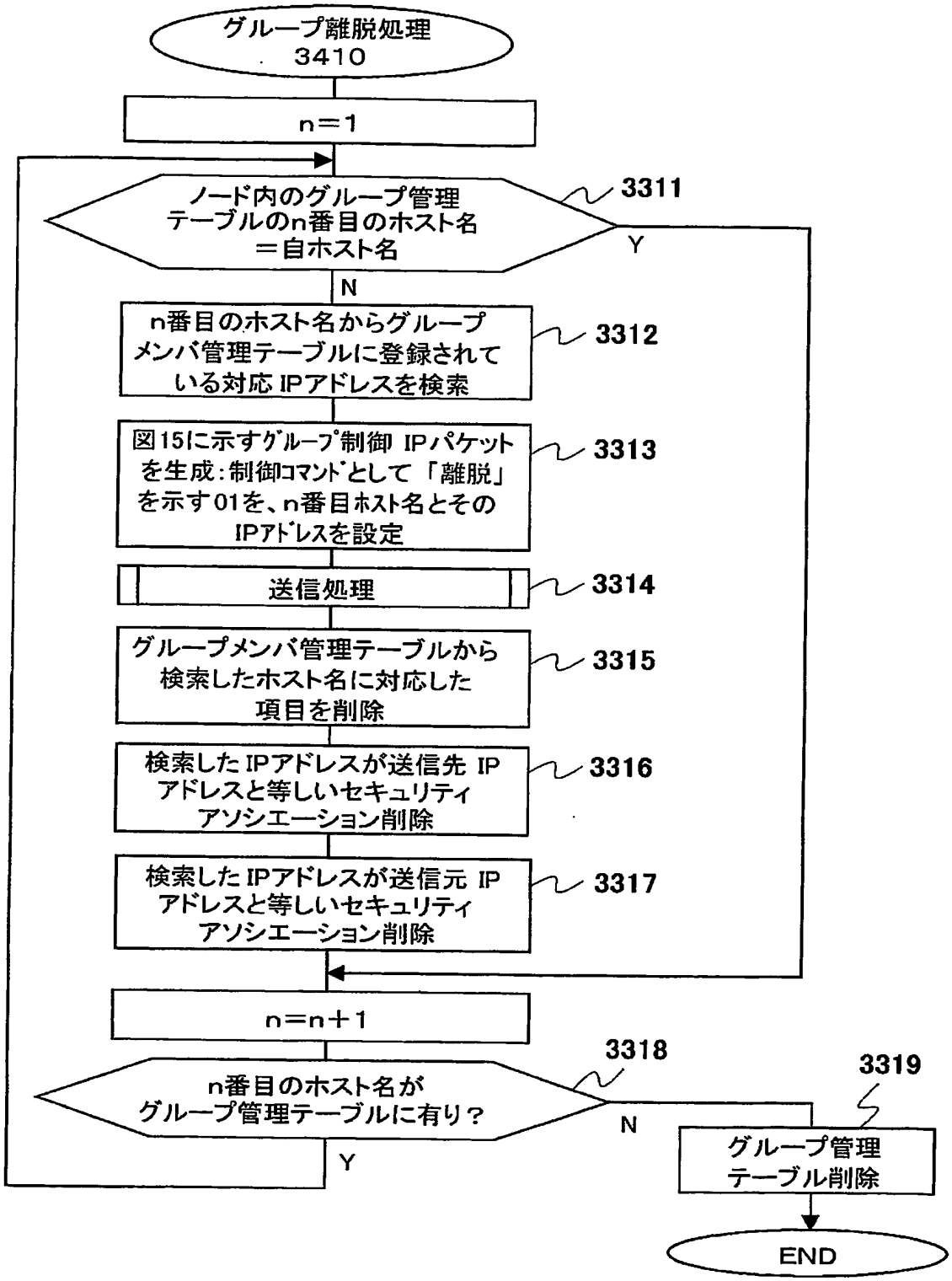
【図１５】

図15


ｸﾞﾙｰﾌﾟ内への
新ﾒﾝﾊﾞ通知処理
3710
n＝1
ノード内のグループ管理
テーブルのn番目のホスト名
＝自ホスト名
3711
Y
N
n番目のホスト名から
IPアドレスを解決
3712
n番目のホスト名と IPアドレス
をｸﾞﾙｰﾌﾟ管理ﾃｰﾌﾞﾙに登録
3713
図15に示すｸﾞﾙｰﾌﾟ制御 IPパケット
を生成:制御ｺﾏﾝﾄﾞとして 「加入」を
示す00を、n番目のﾎｽﾄ名とその
IPｱﾄﾞﾚｽを設定
3714
送信処理
3715
n＝n＋1
3716
n番目のホスト名が
グループ管理テーブルに有り？
3717
N
Y
END

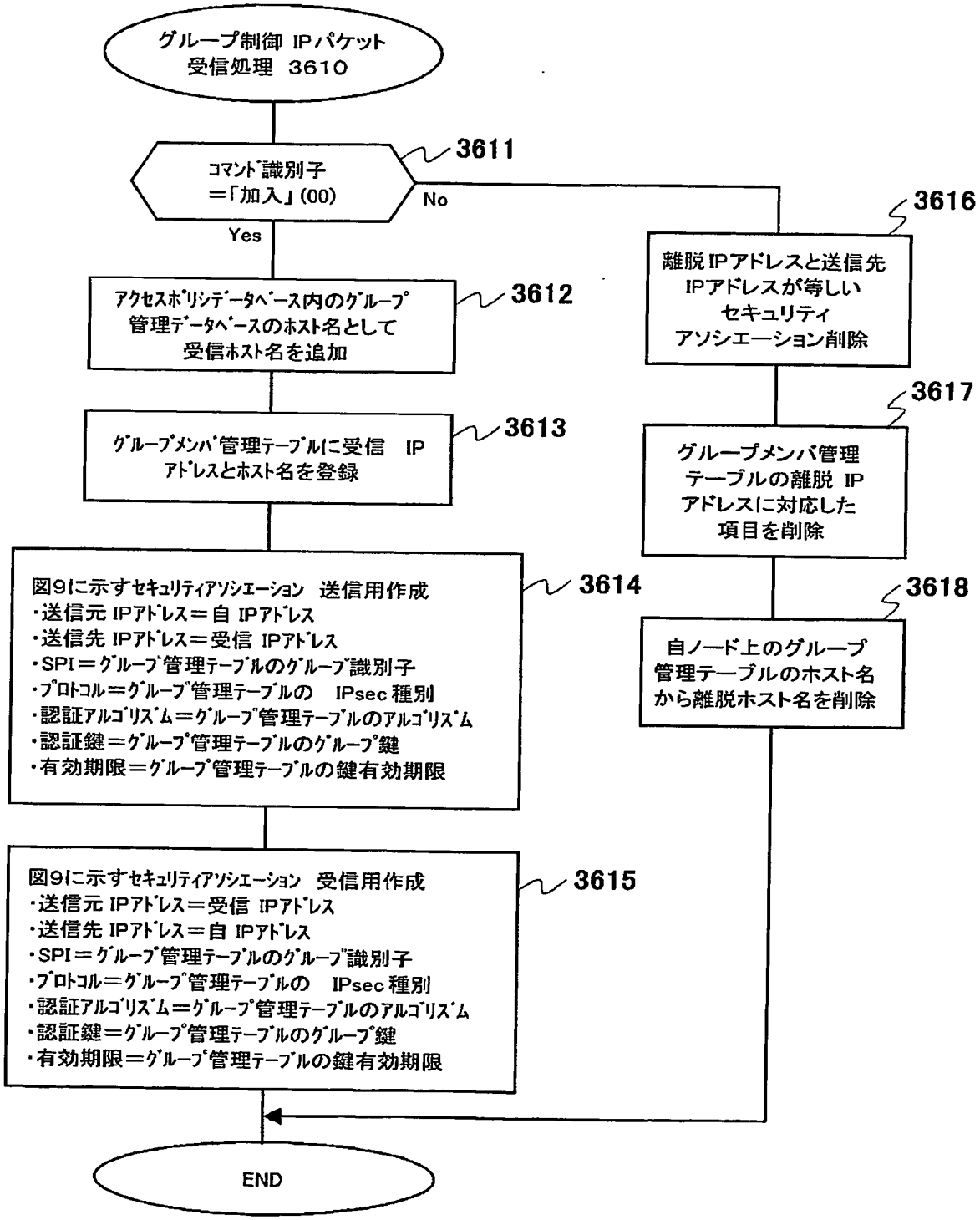
【図１６】

図16


グループ離脱処理
3410
n＝1
ノード内のグループ管理テーブルのn番目のホスト名＝自ホスト名
3311
Y
N
n番目のホスト名からグループメンバ管理テーブルに登録されている対応IPアドレスを検索
3312
図15に示すｸﾞﾙｰﾌﾟ制御 IPパケットを生成:制御ｺﾏﾝﾄﾞとして「離脱」を示す01を、n番目ﾎｽﾄ名とそのIPｱﾄﾞﾚｽを設定
3313
送信処理
3314
グループメンバ管理テーブルから検索したホスト名に対応した項目を削除
3315
検索したIPアドレスが送信先 IPアドレスと等しいセキュリティアソシエーション削除
3316
検索したIPアドレスが送信元 IPアドレスと等しいセキュリティアソシエーション削除
3317
n＝n＋1
n番目のホスト名がグループ管理テーブルに有り？
3318
N
Y
3319
グループ管理テーブル削除
END

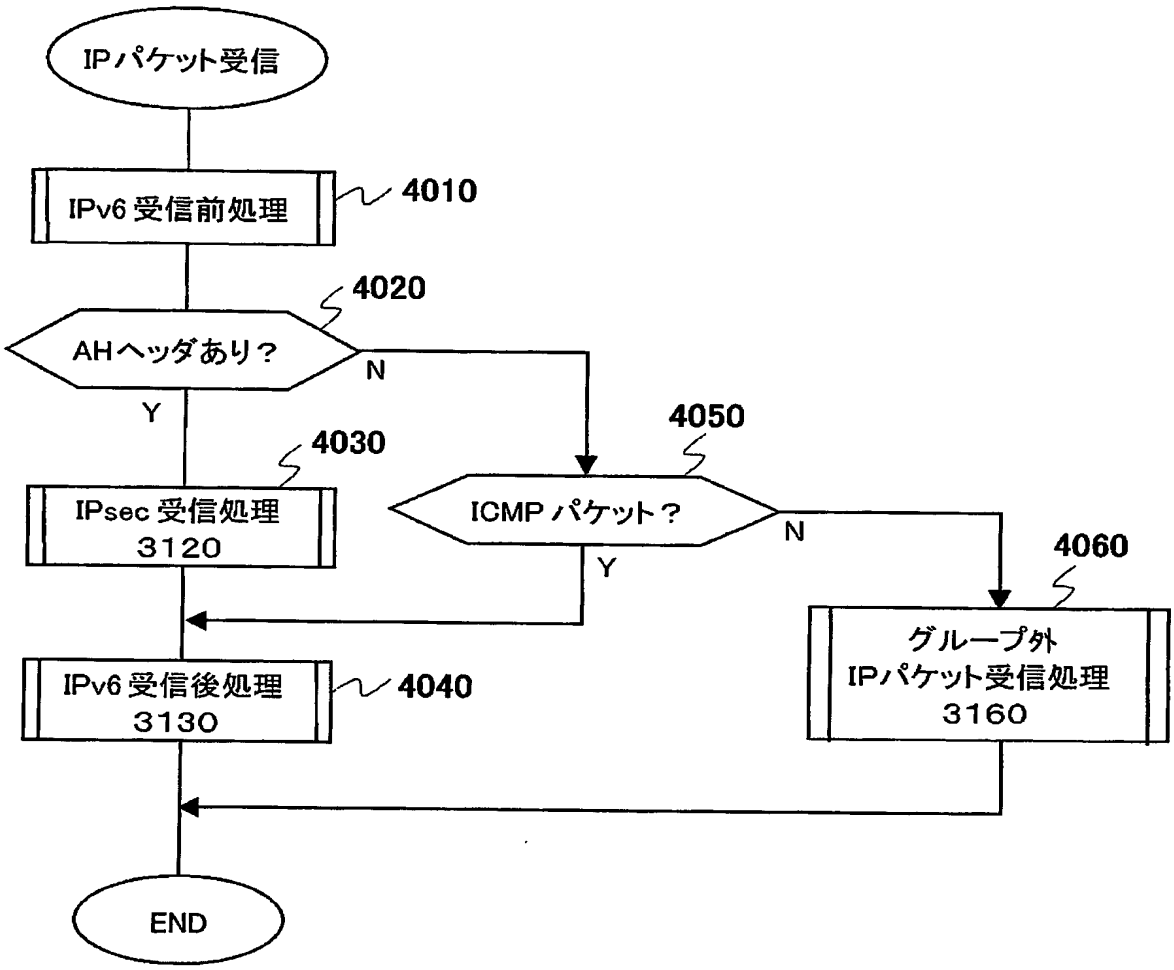
【図１７】

図17


グループ制御 IPパケット
受信処理 3610
コマンド識別子
＝「加入」(00)
3611
No
Yes
3616
離脱IPアドレスと送信先
IPアドレスが等しい
セキュリティ
アソシエーション削除
アクセスポリシデータベース内のグループ
管理データベースのホスト名として
受信ホスト名を追加
3612
3617
グループメンバ管理テーブルに受信 IP
アドレスとホスト名を登録
3613
グループメンバ管理
テーブルの離脱 IP
アドレスに対応した
項目を削除
図9に示すセキュリティアソシエーション 送信用作成
・送信元 IPアドレス＝自 IPアドレス
・送信先 IPアドレス＝受信 IPアドレス
・SPI＝グループ管理テーブルのグループ識別子
・プロトコル＝グループ管理テーブルの IPsec種別
・認証アルゴリズム＝グループ管理テーブルのアルゴリズム
・認証鍵＝グループ管理テーブルのグループ鍵
・有効期限＝グループ管理テーブルの鍵有効期限
3614
3618
自ノード上のグループ
管理テーブルのホスト名
から離脱ホスト名を削除
図9に示すセキュリティアソシエーション 受信用作成
・送信元 IPアドレス＝受信 IPアドレス
・送信先 IPアドレス＝自 IPアドレス
・SPI＝グループ管理テーブルのグループ識別子
・プロトコル＝グループ管理テーブルの IPsec種別
・認証アルゴリズム＝グループ管理テーブルのアルゴリズム
・認証鍵＝グループ管理テーブルのグループ鍵
・有効期限＝グループ管理テーブルの鍵有効期限
3615
END

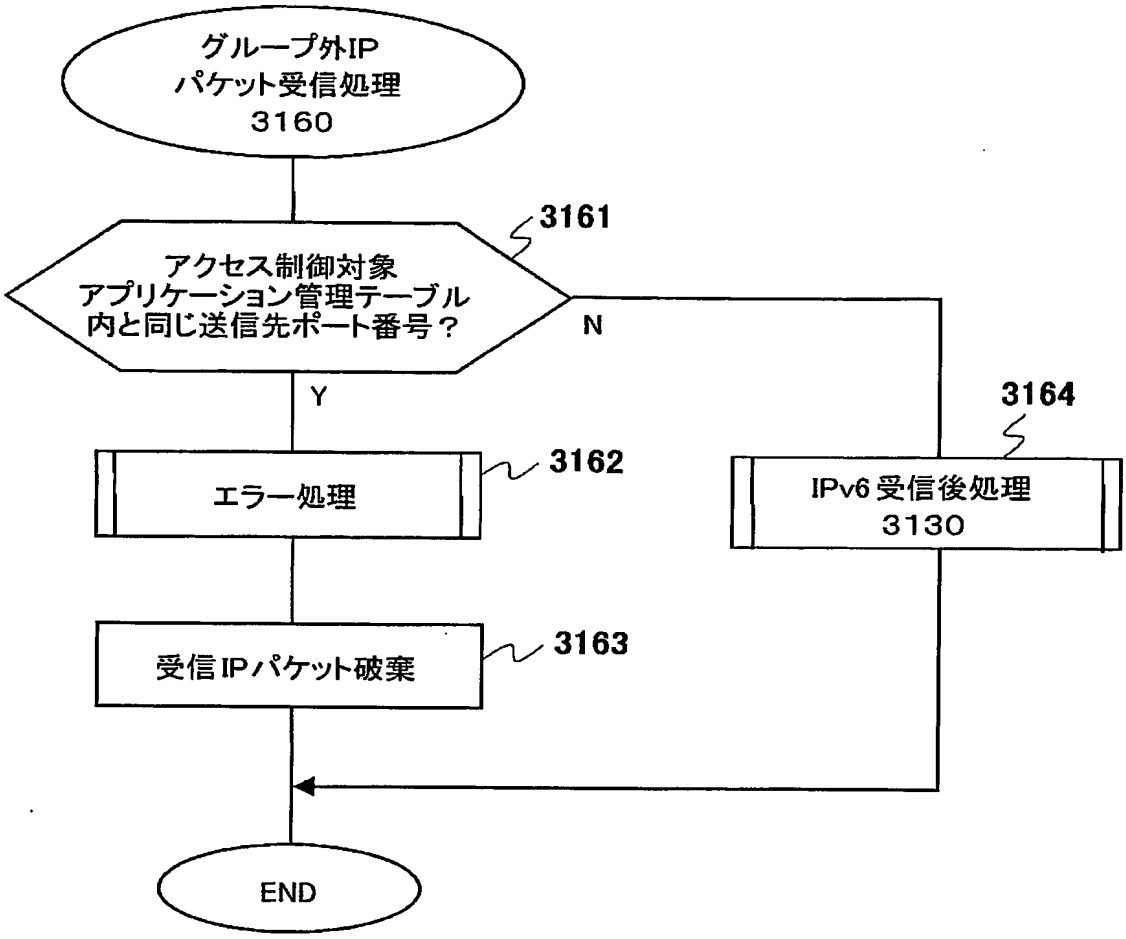
【図１８】

図18


IPパケット受信
IPv6 受信前処理
4010
4020
AHヘッダあり？
N
Y
4030
IPsec 受信処理
3120
4050
ICMP パケット？
N
Y
4060
グループ外
IPパケット受信処理
3160
IPv6 受信後処理
3130
4040
END

【図１９】

図19


グループ外IP
パケット受信処理
3160
3161
アクセス制御対象
アプリケーション管理テーブル
内と同じ送信先ポート番号？
N
Y
3164
3162
エラー処理
IPv6受信後処理
3130
3163
受信IPパケット破棄
END

【書類名】　要約書

【要約】

【課題】

利用者が認めた機器でグループを構成し、グループに属する機器間の安全な通信を実現する。

【解決手段】

グループ管理処理部３０２にて、グループ内の暗号通信に用いる暗号化鍵を作成し、暗号通信に必要な情報とともに自身の記憶部と記録媒体とに格納する。その記録媒体を用いて、暗号通信に必要な情報を受けとった機器は、その情報を用いて既にグループに属している他の機器に自身と暗号通信を行なうために必要な情報を送信する。

グループから離脱する場合は、自身が保有している暗号通信を行なうための情報を削除するとともに、他の機器に自身の離脱を通知し、通知を受けた機器内の離脱する機器に関する情報を削除してもらう。

【選択図】図３

出願人履歴情報

識別番号　[０００００５１０８]

１．変更年月日　１９９０年　８月３１日
[変更理由]　新規登録
住　所　東京都千代田区神田駿河台４丁目６番地
氏　名　株式会社日立製作所